lamps
Internet-Draft
Intended status: Informational
Expires: 6 August 2022

D.K. Gillmor, Ed.
ACLU

2 February 2022

S/MIME Example Keys and Certificates
draft-ietf-lamps-samples-08

Abstract

The S/MIME development community benefits from sharing samples of signed or encrypted data. This document facilitates such collaboration by defining a small set of X.509v3 certificates and keys for use when generating such samples.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 August 2022.

Table of Contents

1. Introduction

The S/MIME ([RFC8551]) development community, in particular the e-mail development community, benefits from sharing samples of signed and/or encrypted data. Often the exact key material used does not matter because the properties being tested pertain to implementation correctness, completeness or interoperability of the overall system. However, without access to the relevant secret key material, a sample is useless.

This document defines a small set of X.509v3 certificates ([RFC5280]) and secret keys for use when generating or operating on such samples.

An example RSA certification authority is supplied, and sample RSA certificates are provided for two "personas", Alice and Bob.

Additionally, an Ed25519 ([RFC8032]) certification authority is supplied, along with sample Ed25519 certificates for two more "personas", Carlos and Dana.

This document focuses narrowly on functional, well-formed identity and key material. It is a starting point that other documents can use to develop sample signed or encrypted messages, test vectors, or other artifacts for improved interoperability.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.2. Terminology

* "Certification Authority" (or "CA") is a party capable of issuing X.509 certificates

* "End-Entity" is a party that is capable of using X.509 certificates (and their corresponding secret key material)

* "Mail User Agent" (or "MUA") is a program that generates or handles [RFC5322] e-mail messages.

1.3. Prior Work

[RFC4134] contains some sample certificates, as well as messages of various S/MIME formats. That older work has unacceptably old algorithm choices that may introduce failures when testing modern systems: in 2019, some tools explicitly mark 1024-bit RSA and 1024-bit DSS as weak.

This earlier document also does not use the now widely-accepted PEM encoding (see [RFC7468]) for the objects, and instead embeds runnable Perl code to extract them from the document.

It also includes examples of messages and other structures which are greater in ambition than this document intends to be.

[RFC8410] includes an example X25519 certificate that is certified with Ed25519, but it appears to be self-issued, and it is not directly useful in testing an S/MIME-capable MUA.

2. Background

2.1. Certificate Usage

These X.509 certificates ([RFC5280]) are designed for use with S/MIME protections ([RFC8551]) for e-mail ([RFC5322]).

In particular, they should be usable with signed and encrypted messages, as part of test suites and interoperability frameworks.

All end-entity and intermediate CA certificates are marked with Certificate Policies from [TEST-POLICY] indicating that they are intended only for use in testing environments. End-entity certificates are marked with policy 2.16.840.1.101.3.2.1.48.1 and intermediate CAs are marked with policy 2.16.840.1.101.3.2.1.48.2.

2.2. Certificate Expiration

The certificates included in this draft expire in 2052. This should be sufficiently far in the future that they will be useful for a few decades. However, when testing tools in the far future (or when playing with clock skew scenarios), care should be taken to consider the certificate validity window.

Due to this lengthy expiration window, these certificates will not be particularly useful to test or evaluate the interaction between certificate expiration and protected messages.

2.3. Certificate Revocation

Because these are expected to be used in test suites or examples, and we do not expect there to be online network services in these use cases, we do not expect these certificates to produce any revocation artifacts.

As a result, none of the certificates include either an OCSP indicator (see id-ad-ocsp as defined in the Authority Information Access X.509 extension in S.4.2.2.1 of [RFC5280]) or a CRL indicator (see the CRL Distribution Points X.509 extension as defined in S.4.2.1.13 of [RFC5280]).

2.4. Using the CA in Test Suites

To use these end-entity certificates in a piece of software (for example, in a test suite or an interoperability matrix), most tools will need to accept either the Example RSA CA (Section 3) or the Example Ed25519 CA (Section 6) as a legitimate root authority.

Note that some tooling behaves differently for certificates validated by "locally-installed root CAs" than for pre-installed "system-level" root CAs). For example, many common implementations of HPKP ([RFC7469]) only applied the designed protections when dealing with a certificate issued by a pre-installed "system-level" root CA, and were disabled when dealing with a certificate issued by a "locally-installed root CA".

To test some tooling specifically, it may be necessary to install the root CA as a "system-level" root CA.

2.5. Certificate Chains

In most real-world examples, X.509 certificates are deployed with a chain of more than one X.509 certificate. In particular, there is typically a long-lived root CA that users' software knows about upon installation, and the end-entity certificate is issued by an intermediate CA, which is in turn issued by the root CA.

The example end-entity certificates in this document can be used with either a simple two-link certificate chain (they are directly certified by their corresponding root CA), or in a three-link chain.

For example, Alice's encryption certificate (Section 4.3, alice.encrypt.crt) can be validated by a peer that directly trusts the Example RSA CA's root cert (Section 3.1, ca.rsa.crt):

```
ca.rsa.crt  alice.encrypt.crt
```

And it can also be validated by a peer that only directly trusts the Example Ed25519 CA's root cert (Section 6.1, ca.25519.crt), via an intermediate cross-signed CA cert (Section 3.3, ca.rsa.cross.crt):

```
ca.25519.crt  ca.rsa.cross.crt  alice.encrypt.crt
```

By omitting the cross-signed CA certs, it should be possible to test a "transvalid" certificate (an end-entity certificate that is supplied without its intermediate certificate) in some configurations.

2.6. Passwords

Each secret key presented in this draft is represented as a PEM-encoded PKCS#8 [RFC5958] object in cleartext form (it has no password).

As such, the secret key objects are not suitable for verifying interoperable password protection schemes.

However, the PKCS#12 [RFC7292] objects do have simple textual passwords, because tooling for dealing with passwordless PKCS#12 objects is underdeveloped at the time of this draft.

2.7. Secret key origins

The secret RSA keys in this document are all deterministically derived using provable prime generation as found in [FIPS186-4], based on known seeds derived via [SHA256] from simple strings. The validation parameters for these derivations are stored in the objects themselves as specified in [RFC8479].

The secret Ed25519 and X25519 keys in this document are all derived by hashing a simple string. The seeds and their derivation are included in the document for informational purposes, and to allow re-creation of the objects from appropriate tooling.

All RSA seeds used are 224 bits long (the first 224 bits of the SHA-256 digest of the origin string), and are represented in hexadecimal.

3. Example RSA Certification Authority

The example RSA Certification Authority has the following information:

* Name: Sample LAMPS RSA Certification Authority

3.1. RSA Certification Authority Root Certificate

This certificate is used to verify certificates issued by the example RSA Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIIDezCCAmOgAwIBAgITcBn0xb/zdaeCQlqp6yZUAGZUCDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowVTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQC2GGPTEFVNdi0LsiQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/Omr
OP3rDCB2SYfBPVwd0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz
+zCuV+gjV83Uvn6wTn39MCmymu7nFPzihcuOnbMYOCdMmUbi1Dm8TX9P6itFR3hi
IHpSKMbkoXlM1837WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlmM
yhBzClmgkyozRSeSrkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3styvcMG
1qUDCAaKx6FZEf7hE9RN6L3bAgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wDgYD
VR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEACDXWlJGjzKadNMPcFlZInZC+Hl7RLrcBDR25jMCXg9yL
IwGVEcNp2fH4+YHTRTGLH81aPADMdUGHgpfcfqwjesavt/mO0T0S0LjJ0RVm93fE
heSNUHUigVR9njTVw2EBz7e2p+v3tOsMnunvm6PIDgHxx0W6mjzMX7lG74bJfo+v
dx+jI/aXt+iih5pi7/2Yu9eTDVu+S52wsnF89BEJeV0r+EmGDxUv47D+5KuQpKM9
U/isXpwC6K/36T8RhhdOQXDq0Mt91TZ4dJTT0m3cmo80zzcxsKMDStZHOOzCBtBq
uIbwWw5Oa72o/Iwg9v+W0WkSBCWEadf/uK+cRicxrQ==
-----END CERTIFICATE-----
```

3.2. RSA Certification Authority Secret Key

This secret key material is used by the example RSA Certification Authority to issue new certificates.

```
-----BEGIN PRIVATE KEY-----
MIIE+wIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQC2GGPTEFVNdi0L
siQ79A0Mz2G+LRJlbX2vNo8STibAnyQ9VzFrGJHjUhRX/OmrOP3rDCB2SYfBPVwd
0CdC6z9qfJkcVxDc1hK+VS9vKncL0IPUYlkJwWuMpXa1Ielz+zCuV+gjV83Uvn6w
Tn39MCmymu7nFPzihcuOnbMYOCdMmUbi1Dm8TX9P6itFR3hiIHpSKMbkoXlM1837
WaFfx57kBIoIuNjKEyPIuK9wGUAeppc5QAHJg95PPEHNHlmMyhBzClmgkyozRSeS
rkxq9XeJKU94lWGaZ0zb4karCur/eiMoCk3YNV8L3stYvcMG1qUDCAaKx6FZEf7h
E9RN6L3bAgMBAAECggEAE3tFhsm7DpgDlro+1Sk1kjbHssR4sOBHb4zrPp6c18PO
6T8gWuBcj1DzOzykNTzaMaDxAia4vuxVJB1mberkNHzTFqyb8bx3ceSEOCT3aoyq
5fiFpR0L6Ba1vgg8RTvNCAIApHNa4pVk0XD8Wq+h7mlUAOYGbie5UO8/P2qWjcOz
+zcheyYXJS/iuu0t2/F0ihEWGcXBmoc8D++n7mKst2jkAHD4wlPN2MgVqnmagpBz
gobFNmCZyZpDS+PPTtQZ1XvdGF5Sodc+Fz+jpWun1kqxDHE4UIZzDA/HAaBgORbm
aEZaVsOs9ZExeqOtqu2fPB7zF/1JKdRk4UJOUxS0OQKBgQDJwonP5RwvO0sYoCiw
zuFcYTmN/hI3R3viKuxr19CH6+mvuIU85ooIHF6TiouZwhk+6+Vk7rcXdS554DT4
2RbVrX/5i/MOzx8c8IIwoZJIasLz+vx8F4n6hyhV65bXN7AIBojMh2dt8tP2MZ/R
VEfsk4mNmO6yKuzyAfjJziCnCQKBgQDnDH9UYUIPkq0PSvViKQFJFCB9BJPFhld2
pIgoziw/JZzM3W3IWU0KWG7UxS0T3xmn3IX6xmWW4vX1/088ybObZWYP0edb61GM
I9DoI5igndLgDwyOL2PFuZh5pqqc09DE+cpJW4nNoudqTNmCrjhmxNCGKgGjlD8z
/OkSccvywwKBgDd0ReajRUziEjDxjF2UbzKx8lzJsX4KIs22GIdHqSRCvlcy80Qa
5WN3ULNiyB350HCP69wDFMXYym5rJoQjPvh6GIuhYKv4V8fffxkYv5kx5uWiXZVJ
7v2x+m8rMqlyv+pkyWLV8KKytHmdiBzD+oTWxF7r4ueLjtaxngzxn93pAoGBAKpR
rR9PnroKHubSE/drUNZFLvnZwPDv6lO8T978tONL372pUT9KjR8eN31DaMpoQOpc
BqvpSoQjBLt1nDysV2krI0RwMIOzAWc0E9C8RMvJ6+RdU50Q1BSyjvLGaKi5AAHk
PTk8cGYVO1BCHGlX8p3XYfw0xQaHxtuVCV8eYgCvAoGBAIZeiVhc0YTJOjUadz+0
vSOzA1arg5k2YCPCGf7z+ijM5rbMk7jrYixD6WMjTOkVLHDsVxMBpbA7GhL7TKy5
cepBH1PVwxEIl8dqN+UoeJeBpnHo/cjJ0iCR9/aMJzI+qiUo3OMDR+UH99NIddKN
i75GRVLAeW0Izgt09EMEiD9joDswOQYKKwYBBAGSCBIIATErMCkGCWCGSAFlAwQC
AgQcpcG3hHYU7WYaawUiNRQotLfwnYzMotmTAt1i6Q==
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed a5c1b7847614ed661a6b0522351428b4b7f09d8ccca2d99302dd62e9. This seed is the first 224 bits of the [SHA256] digest of the string draft-lamps-sample-certs-keygen.ca.rsa.seed.

3.3. RSA Certification Authority Cross-signed Certificate

If an e-mail client only trusts the Ed25519 Certification Authority Root Certificate found in Section 6.1, they can use this intermediate CA certificate to verify any end entity certificate issued by the example RSA Certification Authority.

-----BEGIN CERTIFICATE-----
MIIC5zCCApmgAwIBAgITcTQnnf8DUsvAdvkX7mUemYos7DAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIwOTI3MDY1NDE4WjBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0
aW9uIEF1dGhvcml0eTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALYY
Y9MQVU12LQuyJDv0DQzPYb4tEmVtfa82jxJOJsCfJD1XMWsYkeNSFFf86as4/esM
IHZJh8E9XB3QJ0LrP2p8mRxXENzWEr5VL28qdwvQg9RiWQnBa4yldrUh6XP7MK5X
6CNXzdS+frBOff0wKbKa7ucU/OKFy46dsxg4J0yZRuLUObxNf0/qK0VHeGIgelIo
xuSheUzXzftZoV/HnuQEigi42MoTI8i4r3AZQB6mlzlAAcmD3k88Qc0eWYzKEHMK
WaCTKjNFJ5KuTGr1d4kpT3iVYZpnTNviRqsK6v96IygKTdg1Xwvey3K9wwbWpQMI
BorHoVkR/uET1E3ovdsCAwEAAaN8MHowDwYDVR0TAQH/BAUwAwEB/zAXBgNVHSAE
EDAOMAwGCmCGSAFlAwIBMAIwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBSRMI58
BxcMp/EJKGU2GmccaHb0WTAfBgNVHSMEGDAWgBRropV9uhSb5C0E0Qek0YLkLmuM
tTAFBgMrZXADQQBnQ+0eFP/BBKz8bVELVEPw9WFXwIGnyH7rrmLQJSE5GJmm7cYX
FFJBGyc3NWzlxxyfJLsh0yYh04dxdM8R5hcD
-----END CERTIFICATE-----

4. Alice's Sample Certificates

Alice has the following information:

* Name: Alice Lovelace

* E-mail Address: alice@smime.example

4.1. Alice's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Alice.

```
-----BEGIN CERTIFICATE-----
MIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69PhqzpqP1zANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/
pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwX
urhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVB
DpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2w
ZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peC
rhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQw
DgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roA
KHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhK
E1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqN
sy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1F
hdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0
qyTbY4fgKieUHx/tHuzUszZxJg==
-----END CERTIFICATE-----
```

4.2. Alice’s Signing Private Key Material

This private key material is used by Alice to create signatures.

```
-----BEGIN PRIVATE KEY-----
MIIE+gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQC09InoWDgWPk2a
f0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwO
Rjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z
34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4
xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3
vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3
SeOWwks7AgMBAAECggEAFKD2DG9A1u77q3u3p2WDH3zueTtiqgaT8u8XO+jhOI/+
HzoX9eo8DIJ/b/G3brwHyfh17JFvLH1zbgsn5bghJTz3r+JcZZ5l3srqMV8t8zjI
JEHOKC3szH8gYVKWrIgBAqOt1H9Ti8J2oKk2aymqBFr3ZXpBUCTWpEz2s3FMBUUI
qCEsAJqsdEch+kt43X5kvAom7LC1DHiE6RKfhMEub/LGNHSwY4dmzhaG6p95FJ1h
s8HoURI2ReVpsTadaKd3KoYNc1lcffmwdZs/hFs7xmmwXKMmlonh1mzHqD1/BqeJ
Hc8MP4ueDdyVgIe/uVtlQ9NcRQbuokkDyDYMYV6hzQKBgQD75ahYGFGZznRKtSE3
w/2rUqTYIWxx2PQz5G58PcsTZM89Hj4aZOoLmudHbrTQHluRNcHoXEI62rs0cVPs
D7IlZOLfs+SSTeNEXxD57mjyyufpV65OcNc1mSJAmMX2jWQ8ndnOuWPcc5J6fNvT
au0a7ZBOaeKHnA8XXL3GYilM9QKBgQC35xKi7f2JmGtsYY21tfRuDUm6EjhMW6b7
GWnI9IXF8TGj15s7oDEYvqSPTJdB6PAb/tZwdbj9mB4qj176x1kB/N7GO974O8UP
/PdHkU7duyf5nRq1mrI+yGFHVsGD313rc+akYdKcC207e6IRMST1ZFoznC6qNgpi
nNTuDz4ZbwKBgA5Dd9/dKKm77gvY69Objn6oBFuUsO5VaaaSlcsFOL2VZMLCNqQJ
+NLFZ7k8xJJQVcEIOT2uE7X/csBKdoUUcnL5nnsqVZQPQwI5G937KQgugylMZLte
WmFXlX/w5qzKXtWr3ox9JPFzveSfs1bqZBi1QQmfp0skhBo/jyNvpYUNAoGAMNkw
GhcdQW87GY7QFXQ/ePwOmV49lgrCT/BwKPDKl8l5ZgvfL/ddEzWQgH/XraoyHT2T
uEuM18+QM73hfLt26RBCHGXK1CUMMzL+fAQc7sjH1YXlkleFASg4rrpcrKqoR+KB
YSiayNhAK4yrf+WN66C8VPknbA7us0L1TEbAOAECgYEAtwRiiQwk3BlqENFypyc8
0Q1pxp3U7ciHi8mni0kNcTqe57Y/2o8nY9ISnt1GffMs79YQfRXTRdEm2St6oChI
9Cv5j74LHZXkgEVFfO2Nq/uwSzTZkePk+HoPJo4WtAdokZgRAyyHl0gEae8Rl89e
yBX7dutONALjRZFTrg18CuegOzA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
BBySyJ1DMNPY4x1P3pudD+bp/BQhQd1lpF5bQ28F
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 92c89d4330d3d8e31d4fde9b9d0fe6e9fc142141dd65a45e5b436f05. This seed is the first 224 bits of the [SHA256] digest of the string draft-lamps-sample-certs-keygen.alice.sign.seed.

4.3. Alice's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Alice.

-----BEGIN CERTIFICATE-----
MIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1
lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+
hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV
8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41
/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWf
NEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4Gv
MIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1Ud
EQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQw
DgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAf
BgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOC
AQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LD
sfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzT
jqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps
98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQA
W++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1
nTXl85RHNrVKQK+L0YWY1Q+hWA==
-----END CERTIFICATE-----

4.4. Alice’s Decryption Private Key Material

This private key material is used by Alice to decrypt messages.

```
-----BEGIN PRIVATE KEY-----
MIIE+gIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCalSn6i8Gi44/o
AVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnV
z5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NLFflHUjURca3ynqEB
BV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZ
KGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaU
l/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Y
j7CFSmq1AgMBAAECggEADgxoWEDDRE5yEZ+s7TMw+WH2o+3XOOrryqnsLbOyv34I
wAAUWK7qZyjd9rSDOAtBOgFhQNXYhWZlT+0iHslCIfqJMZ8wy1iFHBCIphoMSWs5
/D+idXrUef5Y23rClBxXH0g1UnSGXnpUH4ehV6p1lvZMh4OJKEoMC4cpyd1SzXrw
+VGCc1+pXv/tTW3Rb2qoWO9JoWY+Epcssrw5N8OFIFODh4QfbLN6pVTt28aQ4pf/
1KhLoapjFzXSYp/jrcNjYJ9qRdSAbZsKOJ2yZ0yqjLHDCDipFty+W0pkUZcJhsgu
Cg1Stt7tKgSvAV/nEjN8e/vA91/AACKBCNcLzEoLgQKBgQC4eTM6BDCzlusXJBK4
SRC/WwUthJZzfOk2Gmwr0DCTRYhWQSDjBfiQNboazHObVPz45qP10fOt2iPEHeX+
VWAXTNrN69M9lEzxygA3s76lAejBR3FbLWkzLYqPB3oZwSIE7CrWHTXJipFWZv+X
FG1R418fnRCUMJ4j85qem5iyqQKBgQDWhQMJu7FC02fr83qsIdLwqhiDtTpwUN3j
qfp7JoEZOxbm3TgM1xPAkrQTUgfr2ZhXGtUwsuKHyifxQEycrTkBOg0gqAfG0fnv
ybyXK6/guctHJQiy64lL39kPuvQkKB+YO60B/oF6zbyFvqanoKXjpspObN3i3yBU
X5/EOu/LLQKBgQCUVwHWeWAgSg+pgBx9jGOnPK4hOCkznRJ7qyuo37Tv+E317lFf
vYFvlYSd4CJmmiUCkZTvK3FkL7HrFo/HwSeQFQEt7aDkN8jX9bPPFv8K+UoNgkGp
LA8YVFrDQSPyadfNVYvsuXhzJLZSYGjPOGHgI5JufYLDZ4UDK/T97ekQYQKBgDDM
ORCxvXTyGiW2USVu3EkaqFDtnMmH27G6LNxuudc/dco2cFWbZ0bbGFN8yYiBCwJl
fDGDv7wb5FIgykypqtn4lpvjHUHA6hX90gShT3TTTsZ0SjJJGgZEeV/2qyq+ZdF/
Ya+ecV26BzR1Vfuzs4jBnCuS4DaHgxcuWW2N6pZRAoGAWTovk3xdtE0TZvDerxUY
l8hX+vwJGy7uZjegi4cFecSkOR4iekVxrEvEGhpNdEB2GqdLgp6Q6GPdalCG2wc4
7pojp/0inc4RtRRf3nZHaTy00bnSe/0y+t0OUbkRMtXhnViVhCcOt6BUcsHupbu2
Adub72KLk+gvASDduuatGjqgOzA5BgorBgEEAZIIEggBMSswKQYJYIZIAWUDBAIC
BBwc90hJ90RfRmxCciUfX5a3f6Bpiz6Ys/Hugge/
-----END PRIVATE KEY-----
```

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 1cf74849f7445f466c4272251f5f96b77fa0698b3e98b3f1ee8207bf. This seed is the first 224 bits of the [SHA256] digest of the string draft-lamps-sample-certs-keygen.alice.encrypt.seed.

4.5. PKCS12 Object for Alice

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 4.1, Section 4.2, Section 4.3, Section 4.4, and Section 3.3.

It is locked with the simple five-letter password alice.

```
-----BEGIN PKCS12-----
MIIX+AIBAzCCF8AGCSqGSIb3DQEHAaCCF7EEghetMIIXqTCCBI8GCSqGSIb3DQEH
BqCCBIAwggR8AgEAMIIEdQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIWQKs
PyUaB9YCAhTCgIIESCsrTOUTY394FyrjkeCBSV1dw7I3o9oZN7N6Ux2KyIamsWiJ
77t7RL1/VSxSBLjVV8Sn5+/o3mFjr5NkyQbWuky33ySVy3HZUdZc2RTooyFEdRi8
x82dzEaVmab7pW4zpoG/IVR6OTizcWJOooGoE0ORim6y2G+iRZ3ePBUq0+8eSNYW
+jIWov9abdFqj9j1bQKj/Hrdje2TCdl6a9sSlTFYvIxBWUdPlZDwvCQqwiCWmXeI
6T9EpZldksDjr5N+zFhSLoRwABGRU8jXSU9AEsem9DFxoqZq8VsQcegQFY6aJcZO
Xel7IECIAgK8nZlKCTzyNVALxeFw0ijWnW4ltDaqcC6GepmuINiqqdD94YAOHxRl
1lKU4mLknSJ36W4T7vaI4fp98sK0nGpaDzQheu6BbQ+dVd44q52MDwvqvD0Y7UjF
IVEP3V9Ebfn641CR0mIcVCUynxb3aaKjhgBKTGbYsKtPue974rDPIArMs2Heo8y3
cq+f7Jce0IVCglRatN6rSyJBF8JlBQW5pZGco8AwTM1pK3RrdIDziheA8DIBB+KT
4JZBO6UprlcZ5wBY6ncXWa5E4feb57Cd3bB+zJuubBX9f4yG/J0cSF59w92c/6Qb
i4EFk6tAiz19PxuLLwjco71e69Jiav19Ph/WJpf/XCEurw7K+VAeZALFW41G/D30
WIBRC2shisHB3j8+3fNPcvi4Fy3EkZNW4lrZFAjbBtloCxk5rcfRS7vxucAvC5X9
4bm0xEcdOysnuplH77u+CWWxjCk414SlKZTUbwc1a0B6yRDvojUMZkDzMqsxyYjn
JG5QhMFQrTyALwCgJsP/rAf5xPhG2p+9Qul0yiBIIZwvKNKRQKL+YLcvYvTh1bhj
rUflYzzvviyXCy9LcX2GBop9yBFJzIcmKfL0MGua6WIkWX2BIjhGTtu6VThmRHuf
OsqNg/ZrNCTYa7e1D6gwP5uFRecSZdASf+0XTe6M7e/vaN4Go4A3H8+d53SYQP6n
pTt/a0DTHzY77aNMh+mzkIHC1W3zUdlS48tUyJMiAN3Tt+RfhHZfgloJ7IdcYdM2
O1I+UD/5L9ghxN8dh13Fi3rDyn6Y5xB1xFuZ0mLjoEI+3Pr1+B9Kgf+o/hxFttfx
1uP1XcHt0a4gBr6g7fwGNssfw5S6g6hS9UDTAYOpvLaatil2TZmeYZzij19ssv36
kr1VaRV9xcQCbY05ucD+buymFXPn/rhVdxhgIydmvOtdzDozy0WFDTvgjUBNeRnC
eMVD6AlWdWOlmBqOcIlJS0aY2FWm8Kju62XZA8YIRowlLysuq3zIqDmzmqJFKwuA
mRMZmUVhophMEn86rwob3Z87gNbyy1U/dXi+s6Vybx/kiwDXjfyhWBnhn1gkhgiv
oOhGtt+yAliCVuHQlEloQeQN04C5QTU0d1WOj489Ft6wpvm0tqcl6NpnRYUhbCoF
XhFr4wswggR3BgkqhkiG9w0BBwagggRoMIIEZAIBADCCBF0GCSqGSIb3DQEHATAc
BgoqhkiG9w0BDAEDMA4ECPoEFEHQGB9dAgIU5oCCBDAOrGHyN47xktt1J1VvWQZN
BYIMFzLN6p2/zKotGf7EMdgSdwlxkhKTWxunfoP/gfRD6boXTAA7ukJDsHXZrfXF
KjI4HI2oa/NihwqctphcLonBJXcofuHv+loP9MPLtwu3Mo1wsWTiHpf5XmxMoZQw
fbrp2ohLugJO1ZRB9RfAUpaAhtFg91pLOtXEpz7GULEyOnYh9R8iu9bSel8bpl4S
+AoxzXD4gYiEU6Yi0/47aRstd3H4u3ERDnUKSoqVstslRSKnK/WrGYUwoy7kNDwy
DBitfosMY0rpWEe5rXTBwJkBodcl3LBpDbNzdbrZw+e+yObJ9zfRlMpl0xVfoiji
q9UbRdgN2yo0RKwF6c63V2RdF5tjQHnNIM3K3tC9zEis11jgn9LeOLB9Cd1qyE4P
WfmHN0gwqDF1eX96TmUipmYM63H6jcbnSc6p7eIZtCrqGjhsTqFwcMg04WaXWeHD
ffLXSZdzIUB+zfC8tftUUEOUX3tX4l1oU7K8uAuQTSK/AXwUj+MbQVhlz8te4FVr
w4ulZ184IYqhD3VdIOxXiZkfSKChRz8/7QacrXFvfKkrcrxS2iHMoxhoJ7WETNtI
slW5R5runj61r50VT4HCFNFQfGBbTtV9AdP7yka9aQDWxPCoXFgeb1Q01F/BigzW
02JP5Lcrw7ia0y88QbTzWhi57d4he5OIp0wHUiGPh7s792mlltvuSpRKJkOXWv6h
qAj5AsBB8JNvgXP71Ytx2vMdjw6gqzQcxASJ4UHQg0CxmiODLUP+FHAY1CPNSjbR
pHrTi1UFi/+9hYneQci++qPvkCqMuGHVxamd4OLanGJN1NxE1DyMeduapX5rXuPn
g66LPey9GQuE3SBNC2dmjuOy7d8fWXEZqhqLtPfsuwVzdnWb1uAcjRfQPNo+uWe4
zihYisXK3lqA557dRqdSv+6GL6/OZQOCTaYMyZIWD9jS2gU6T3q2j8uk1LNcL9n8
aSpQ5xWspBXpzXo39fG6CMeqzZlFCqrvQwYhdXbtxn9Ox/pimmWOlcqAxv+xythW
BMx+il1JEdbCj015wjmsCWNPWlM4AVSholpZhs9Mq6rvgBXi1HJgjD0DpSLCE0xh
/GNoXoOX3LrxfCIDEhT8LyZ2NE59yh3t6pm88soFzaAghdjb1Fkc79nBbcl4NLKg
SmL/7GktkxEznOiSYfnfJ905kjZC08d8RnoGfrDDUWD2ZIhbbxOCq4E3E0Zt13aH
JOXRBOZLC9L2JNeSNiBZZGykh+Pi4TsIzXL2UPQ+dy4DDaEf8yamyY04dlhFsnhD
```

```
qr94Y9E3O/rpF0yUb2gCehEgT9nppVuMeridsCkHqemmgVr/52Xv/XK9dx4+YBjL
4/3Id0/yVJURqDIHH8o4ogF4rflkzOalrZ9nJFugP0UM8oNysaL9yr7/Dli1juV0
MIIDZwYJKoZIhvcNAQcGoIIDWDCCA1QCAQAwggNNBgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAzAOBAidIqBxZFwvagICFCKAggMgTzrUv4/12Jqnv3AL+P6990uX1ybZ
NcTwC+hMRV0Ho0FuAAybzdSRBAaZch1+8GheU8yz7IYWmLn1PNHxlZ8inIYfmTfk
Pa34Rk8s/RxJIe8LMYL1qjk/FMq/Fpgc0S65S6bXvJ69Hb8gtAoGW8P1b0dd9bvG
NbAk00h5r+IWiH4U8zGpcqWDWRgieGICsY00Hvx4KKMV6FIjFVCTZevORVoyzmSX
ZZgxqrbjw4CZqOWReHPI3aEt5xVX3BihRGi4EIyia6yU10VOZTGBKqWUeKmOA5Gw
SX3mH/kLiya3gwwGvdq1ncXcl7V1STN1HFyp4ebGKg4CsZ6NkWjocwq2PwM/TqoZ
5i02tqvOeR8lX7LrSegxGH81Kw3nMV4dH5txoVt9hddZCKKGcJ5Z8FlzxFP4BFuF
7hOmRpUPdxiahJ/GkXDVIAw6BJKd4Q9e6sjJYxTeq4uOP6V4PMuDU7F98X/d9sEx
2X3b1cJxuA7xtOnKAPsWEyWBg98B+CKG6KwO5s8TlZVmlk15FCUjvFoKCiWIKF4N
vGLiWOIP/jJ9N6Gqp4gNbm51zNFGZ7gZAtvsBSGQSOUPgfZcx2mRxpBmcX8tm5YJ
hmY9EDK13umUUGKrPOrG8c7/MVAQegSKqQuXSfMK6KknXGe7jwjs7xaQaRm9fFHS
0KbGU3MsLxRGjW/jzjUNAEWDiSYPCVo8E/kd8LETvjAowF772y9o0X1ZzcP7HWcl
oYcO/WSSh4e+FAbgqLo/8KIkGzJ23BAcdx8XAtxzUZhRdHaItnwaJsfTr4TCwq8C
XxJG5u44/z6imqQrVOaXQfvk6ssSNGdG62TkacYg2K63D9hcg+TbZPPVSStWXyj8S
N84anzTOxb1yx6aw6IL+uBLC4jISgNFijaF5pwjLSbgTs5Z7skZdCam80xYmdJVO
ES/uqFCQFUSamXXNbotviQk8jWuJFz+BXzPYJN3t+3mp6SmgTZ2zP8FUQEE4GbSH
DqYV621DcWRo/mao8xzX/mvkKm4ddGBldiusoHZaL4gdo2A1qThSMnMBsciC+jEj
DqOr70XhHccTDW8wggWUBgkqhkiG9w0BBwGgggWFBIIFgTCCBX0wggV5BgsqhkiG
9w0BDAoBAqCCBSYwggUiMBwGCiqGSIb3DQEMAQMwDgQIehcRLmVUApMCAhQOBIIF
AHb5dXZKzCeRUo2ZSj0oyuFS3zQ5HhKyfapsyCqbYCKv/lSzNYWvuda7xfa+uOM7
/wCB9sWdz0MTpaBMHWx9hvibZIY65oM+ry4tTuKKqOJl37OsnjB0dSNTKszsI3fa
PUjslxqIH3aC1shD7OqhIRGZzRjK44PJyWv626oQrgVtTYR9NYTdee+SbBZbkEt/
EpWipwftWXGR6tSYJQn99eO9Vih8HyQvwIpidUh3pCFOlow4VZyAqIWOHcw9TAjB
XNv+qfdH7fiX9wM5/GvnQReIsqjXCUoc6pSQIAqD/f+I/d1F2ZmqM7KwX0LGRER9
OWZGyF734pN9GLbNetWm6rKxmlSI/5m6+2Jxxfann16P+vBSEgWJ/I8GnJAdzIbB
Tyfjog4Gi2+lmrPzK7+C79ntM9nfsr4xVzy/BknwZIaJksd4VvOGkS9nfM6shtBJ
B9uR+GJfthtsvIVUHN0kz2r/lVzMSRbOg9yR53hv1H/nXCmUjWz/BvobmoaVBcCm
mOnnYZTHMNarIVYdLQFif5ZLH7WV/XVEVIoRntNRiKsK96VAHm5XboWQGCqL0heh
IX3Nily1genGm1aFlSQNMvLDko1ILDTKrINvPmjG/WFoLntpJFPtYZsooT1jjXLw
3VTSodtgKQNdPYOEidSJqwIS87fzrCB2Wmwys0iGfdsuNhSaqNqa0dMO6FiW2fku
x7H+w7SX1/n9YeZUNLOcewLcC7E8IA1IarjglZE1L6Yb2ldXxV9q3PPOwKuGnah0
TKnD6mLn5BIGOGTzF1VspXRrJhFrcLe+xsJR1r6niI3bcMWXXy7gbm1X/CRE902I
ynxE1oDR+xZ6rjPWDJP7kVf4GvA8trCGrot4pbJbmwlBeMIylScdQoHEnyqrenOn
RMmXZaKzl3njtq7Wk78qoJq0a6Vh/sde0KcOPFkyTZdMBlTztm0K2VJU3jUVzPlM
0WY2fyGDoA89ol+/MiNsgiaEghGybXBYipOex+p7j1GIRN/CKmpWsqjZnB78kyXm
Z6AE1vC6neD/7zANInDkzXiun6ic72LoBX3JGiCSuM6hIPJ0AcDwlzTDu0H2rCQN
w+tivJ2v4KbgeKoc6beQb5fZHs7VsWHikIcpwqB5ngwt34wHgFG0nTS4lZmvzSJ7
FMRVGmsDYkDTpZzgNOaxiUBQMcEvxNIe3nAmA+dvB7w6XRQVSUsL+vBFhHiWGZ7h
k5sCeHElewXK0SyJADgfFlYq3EfEgZ13h4wtoSfbBVtzbbyg2LNegUCLfIJkc7fm
T7X7JSxbjOgndMHEeMdVb+NFxbgsXYrYD8rC2A8l5cQzZrsxb1bvgybEJz+NU/52
UgGrPmdjJKuGBK/V2zor6qPvKyId1Gb4QQuIoyClwhZ+qk9nE4Eft84y7ISgMywH
+lw87HrSHKfpqzQhCxlrLu53IYK/4PhE7BYC9Q4tvIsZXSGZ+nju4tyzERSlaNe5
njUeIENr4B/+kXULwVDcvMFHqUFJMkFai8FUga7gyipZ+654clGgJjnNBO1va8Jc
dtdPRRW4gwdrVn8u8J78KBzt6ChkrpKRV8VeWKBk9lhcT0ZNpJnNqhDrkfzHBqP0
Uo133I7P7C+h9sNDI153W6IOIodyQE0Av1WxHo4y/1d1VeGDaB7hOSDq9ZMpm9n1
```

```
En7F6/1/s4IUZHja/qRrK9hD4M0Xq0LhFXuUzuipo49OMUAwGQYJKoZIhvcNAQkU
MQweCgBhAGwAaQBjAGUwIwYJKoZIhvcNAQkVMRYEFKJTQdVEPIApFXwBI/Dnjq/N
83cPMIIFlAYJKoZIhvcNAQcBoIIFhQSCBYEwggV9MIIFeQYLKoZIhvcNAQwKAQKg
ggUmMIIFIjAcBgoqhkiG9w0BDAEDMA4ECKq4DtyiayOyAgIUpQSCBQAKQtkPOS4s
LE6Os7nP4RaJWBuyXl27V/o6TusBRBgQoPzP+aC+O99wgisEKedyB47bAzcO4sba
4q8UkERAsYHcEhdD2hGRCL7ou9jTtrr4RgZpa5V9CJcBO0t4bqy2lUefOpm6no+R
X840uyM4q5Q+cfH1rTQ1a/a+gLglbptoEkH/4dfR3ELYiXcM5UrBYTJOHcyME8c+
TXbpf7kiplTtlsrlZyU5zrWcxngrBxwFA+O85W/uVR3QZSW+EGx/VCYwGruZlNyt
BvBYjsYsnC+yKYXbqL81DgOePy+eh6VX64SwBLXcWcY+NK2EZrhzrUFjl+PXFKY3
IVVPJhTE9o7gJA0hzvAanOluWXozD3/WPQaXhyIJDwM2MjznjL2MBydpy9K8Cio7
XaV6PX8DszIZkfI4DAz5f7G7WbwUq3IjPPPWiUv+JsR+dnqzWDJ22SXc+AdQP2sK
qMvP8gOpHOsVlXXE76c5rUcZCZD+gGv1avO7YttWqbDqLj6oQEIJ8LX0Qvwd0YEh
etE0bJ5uv2njhQDhLkH/JIbmFSgJZeM8dtKHb8f5wZc2B+nXGB+TFboGzSuP7gaW
u1vKsJNqT/J/FYEqcamI2F+td7z1sGfbR9ckAcxXeb2uPVbCJ1a50gRlz9qVm5Hb
5f53X7aoQQp3F3LDGQmJ+GFQ/oXXwabqn4TvNO9KDhxpGcMMU9RnugUfNU9GBec0
vfrzmVKZdmJ36HOmMnLvgRakRhCV3kGABXY83hwUv17E1qASLKcAWIachkCCGpBG
yGtP2IOZTn7PsLJR1BzKnePa7MgFcgoCToIpdQnCTtAsalmBm1s480LN3GB5ojeG
bQvNf9TAviA0tg5VuT4/O48V6uYSJsIZsawm3tGA/LjxyfV1aLddQT5Zf5ZX9BX+
K/PB4oYAFxtUpMK/aL5G1MvppUJ9CjqAtnoKE+EkdQmyZ1VoDO9ih44zuRx6XV4A
EYafNB8ygjRHGsvPW0/M0Es0w16wzJHTuf/15fD/nH7Xh5MzhCF0CtvLn8v+S1Po
i2/40O6pS2byjUFRbeCpzEpRxdv90LCb9ALdy0yG9u41W3yInKNFnaWBulfOPFCe
ZT92M1BgwJA8ZcydtiiunRNAH5iWLSPloUpOD1v6En+rat+PoyRXIy2fLHBL25aw
LhABoZPgRsCiLsiNiohfyngksrQKeRgOlaBMT92J8r1E4sUKirQlcOdiWBE6vmBS
XzyN/twvfgPNIXgR0rw6c7VhhS+hNTrsttg/xcfvJ/bftDbKm+RZL+yQoOkkAf9R
5tizyMdMBlaMrpfrBxvNtMiykbZ88SYoA70Trwab2aHQluVhs8OjXGBEOqmSudcS
dV1EhBpo9HBsDZZi0IwOp5/B9fCHdnThCTiUm80eQ6mX2/DB9LlNh7gHOyLL3azT
m12D0ZpZNaXyxLzdiRiAdwpWZmmegOOG70yi0D5eIxh6cbnbuU6Ygdp+pFFVYHfA
vc5Czpne2OPhXX2k0Okbwawr9AfrFjIfAEmBFx5GBGr/lSiUQSkbUC/s209YgaOg
WTYt3KXPzrThJJGZnnXZRTGfIi6vp8RsnPX35+Dxe/Lp3gXDdIJeWG6XVA8t3fsp
coTqPkm/XGNMmOZ81KX/ReVdP+dC93sov2DuDZbYGPmHlD47bOOiA68GD64DEuNt
Q8MhWk8VRR1FqcuwB0T0bc+SIKEINkvYmDFAMBkGCSqGSIb3DQEJFDEMHgoAYQBs
AGkAYwBlMCMGCSqGSIb3DQEJFTEWBBS79syyLR0GEhyXrilqkBDTIGZmczAvMB8w
BwYFKw4DAhoEFO/nnMx9hi1oZ0S+JkJAu+H3/jPzBAj1OQCGvaJQwQICKAA=
-----END PKCS12-----
```

5. Bob’s Sample

Bob has the following information:

* Name: Bob Babbage

* E-mail Address: bob@smime.example

5.1. Bob’s Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Bob.

```
-----BEGIN CERTIFICATE-----
MIIDyjCCArKgAwIBAgITaqOkD33fBy/kGaVsmPv8LghbwzANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowODENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5nAF0glRof9NjBKke6g+7RLrOgRfwQjcH+2z
m0Af67FJRNrEwTuOutlWamUA3p9+wb7XqizVHOQhVesjwgp8PJpo8Adm8ar84d2t
tey1OVdxaCJuNe7SJjfrwShB6NvAm7S8CDG3+EapkO9fzn2pWwaREQ6twWtHi1QT
51PduRtiQ1oqsuJk8LBDgUMZlKUsaXfF8GKzJlGuaLRl5/3Kfr9+b6VkCDuxTZYL
Zxt6+a3/QkaC3I9m2ygPubtHFJB5P5+s8boROSKm1OB1gsLow8eF9S7OtcGGeooZ
JiJUQCR14NaU5bIyfKEZV2YStXwdztoEJJ2fRURIK+8YnwlB3QIDAQABo4GtMIGq
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMBwGA1UdEQQV
MBOBEWJvYkBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQUF8WEe9Cn73aQOLizbwi8krWeK5QwHwYDVR0j
BBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAG7e
QY6Px7WZC5vCbF5hjOitxoz3oyM+LRcSTGWoYXdmlwsNUzy31pE3dtADvevRtsP8
uN7xyfK6XZBzhShA/BtkkqYGiFvXDpluOxWmqC0WPmc1PNK2mHil+pGMfvnUwnxd
6gKcHED5p+bUhDyIH2fy9hGyeOUs8nvi+7/HwBipN+nA/PfsPn+aU4l1K6qDoG/i
kwyuiWcFFlc5yE5rkAe2J0/a4+HtzNmTK4jB/4GbyI6xlUszPlEqKE+Es10Xut/y
UWL5nKKaqpRRd07Pq371MpFQs2+zXt4fGheKzZU3XXrIPcAPyJjWiyU1DzpqgSJM
OIp/HtXdFscHb9+Qic8=
-----END CERTIFICATE-----
```

5.2. Bob’s Signing Private Key Material

This private key material is used by Bob to create signatures.

-----BEGIN PRIVATE KEY-----
MIIE+wIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDmcAXSCVGh/02M
EqR7qD7tEus6BF/BCNwf7bObQB/rsUlE2sTBO4662VZqZQDen37BvteqLNUc5CFV
6yPCCnw8mmjwB2bxqvzh3a217LU5V3FoIm417tImN+vBKEHo28CbtLwIMbf4RqmQ
71/OfalbBpERDq3Ba0eLVBPnU925G2JDWiqy4mTwsEOBQxmUpSxpd8XwYrMmUa5o
tGXn/cp+v35vpWQIO7FNlgtnG3r5rf9CRoLcj2bbKA+5u0cUkHk/n6zxuhE5IqbU
4HWCwujDx4X1Ls61wYZ6ihkmIlRAJHXg1pTlsjJ8oRlXZhK1fB3O2gQknZ9FREgr
7xifCUHdAgMBAAECggEABcQg1fTtieZ+O/aNdU149NK0qx97GLTBjIguQEDDBVFK
2lu4PhBg9AdgAUqLH1PE+eq65JaGZwvFH8X1Ms2AKiRzYsPOQIoJ4n1hc69uiEN9
Ykcv4QHOvvqtCtWYjJyb5By9WPeLH6QynJ6FlBoSqxhURSWyYfTuwqt1OHEhsUuH
d3N5BmbFiRBNj4aIA9zz+i5xL0m33kMKai/Ajj3sI0AJsZ5ZVAhYbC8sCt1Xevb6
i41p9S6GSwGC19by+1y9WC1QGtb5GDotvChMvmZS/O3NeDc6xC/LZoQcHNVgiZd7
f1g6iEkJlCYK+D7xsd7Y630w75Haj0vnlhiJObSA+wKBgQDxv8jp2D6IVRGgYfaC
nUU3Mg70wagX1fgPHO9Sk6e9c8CgORh2uwWjpTawu88xBGFyZ+xnWqr7GCNsltas
3m94ri4A4R94+5uL8+oOLC26gMDfzATd1Q3k/h919YLk89tonQEUbCFZJdphThEb
vg2W+nNsEVcQGuClzhX0AyGMswKBgQD0BYk3sdGQbBA/hYD1EYsZfYebUiYv2lTt
VGRgTohKFclRAWOtGP9YRbKyEVkBLhjgkXzS9xGqKywP71z9Iny+zDGbzk8ElB/g
lS7GFGX50TG0ISfaFWTYdxt4mN9pduZE2blT/26uyU8DXCEBhF/OqhwQjJqKTYTT
Rl3Ara5fLwKBgQDQyVtjIyD2q8naY2D8c4mo3vHtzyc21tQzcUD8Z4vSYps1hbos
KN/48qJmRv3tjqP+o+SXasYKsFE/4pIroLxTVNNkbQm6ektfttwpO1yPG834OwLk
97HVWOig/tX6mOWg1yBsm+q9TKTrrvm1pRGlmE6BQgSYYy4r5O4u3VlnYwKBgQCl
B4FvWyDhTVQHwaAfHUg3av/k+T++KSg6gVKJF1Nw1x8ZW5kvnbJC3pAlgTnyZFyK
s5n5iwI1VZEtDbKTt1kqKCp8tqAV9p9AYWQKrgzxUJsOuUWcZc+X3aWEf87IIpNE
iQKfXiZaquZ23T2tKvsoZz8nqg9x7U8hG3uYLV26HQKBgCOJ/C21yW25NwZ5FUdh
PsQmVH7+YydJaLzHS/c7PrOgQFRMdejvAku/eYJbKbUv7qsJFIG4i/IG0CfVmu/B
ax5fbfYZtoB/0zxWaLkIEStVWaKrSKRdTrNzTAOreeJKsY4RNp6rvmpgojbmIGA1
Tg8Mup0xQ8F4d28rtUeynHxzoDswOQYKKwYBBAGSCBIIATErMCkGCWCGSAFlAwQC
AgQc9K+qy7VHPzYOBqwy4AGI/kFzrhXJm88EOouPbg==
-----END PRIVATE KEY-----

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed f4afaacbb5473f360e06ac32e00188fe4173ae15c99bcf043a8b8f6e. This seed is the first 224 bits of the [SHA256] digest of the string draft-lamps-sample-certs-keygen.bob.sign.seed.

5.3. Bob's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Bob.

```
-----BEGIN CERTIFICATE-----
MIIDyjCCArKgAwIBAgITMHxHQA+GJjocYtLrgy+WwNeGlDANBgkqhkiG9w0BAQ0F
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTEx
MjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowODENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxFDASBgNVBAMTC0JvYiBCYWJiYWdlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAqtHAlBNMiBIk8iJqwHk/yDoFWwj8P9Z1uYdq
1aqIuofvjoAyjdA8TbsBRGdmvaIOSQOepsNjW1ko7lE8HlDs9JHn1E+tzH3mKfn+
G2erY+alkMJTXPvMAUdCA8+e1OJ7k91gYXDpzIWrP3Kc0xTlsJ8tGJ6mhydJX3wP
0/HuyHpfKQQfDusPH8S5yidPciWuB7Wj0X4xY1pUAz2rSSAlnGvhEzKFbW43BPjY
XPUnRWMtXFya1djq6Eb9M/klbhdZheDLLsjLUSXYU70r9VXGM/qcjd/NhWYphCeB
cqswaM5mXLYdm0mFmqoecF62mUE0DiNdhwKTtnefd0cll+D3FQIDAQABo4GtMIGq
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMBwGA1UdEQQV
MBOBEWJvYkBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIFIDAdBgNVHQ4EFgQUSrOsMVMCSZxN42554CVhlT6IYiUwHwYDVR0j
BBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAC2c
Y8FgaxgB+Dx9gAFj35ae1vgzYiWI3Ax3FSxogo/GzpK//LB4215oeBuKXbm0ixBn
4nojxD7PMlM0i+ilAvVNJNaHY9TtgIgq8V/C0C7vL8SdBN01e5ZRI764ohu9ivYv
Ixvvt7gzvSTpe+NUT1i09xNgsC8v19WB/BwkqMAgDqMxqCxT4fyrvVwpxNBke75j
E6Q3xCjfdOWYcfMLK7EsTSgimYuonZjN7v/yqTdjn/iVH+agL/2MlSfiU36w/Yf1
7EM09uKGH/Javh+2Vjd0j8rE/q2Iaac5VI91M6xz5oDZUknycBKKinR+nJWMt5AK
UAaL2Mjl3YtrUGBpxxY=
-----END CERTIFICATE-----
```

5.4. Bob’s Decryption Private Key Material

This private key material is used by Bob to decrypt messages.

-----BEGIN PRIVATE KEY-----
MIIE/AIBADANBgkqhkiG9w0BAQEFAASCBKkwggSlAgEAAoIBAQCq0cCUE0yIEiTy
ImrAeT/IOgVbCPw/1nW5h2rVqoi6h++OgDKN0DxNuwFEZ2a9og5JA56mw2NbWSju
UTweUOz0kefUT63MfeYp+f4bZ6tj5qWQwlNc+8wBR0IDz57U4nuT3WBhcOnMhas/
cpzTFOWwny0YnqaHJ0lffA/T8e7Iel8pBB8O6w8fxLnKJ09yJa4HtaPRfjFjWlQD
PatJICWca+ETMoVtbjcE+Nhc9SdFYy1cXJrV2OroRv0z+SVuF1mF4MsuyMtRJdhT
vSv1VcYz+pyN382FZimEJ4FyqzBozmZcth2bSYWaqh5wXraZQTQOI12HApO2d593
RyWX4PcVAgMBAAECggEAEvPt6aAQjEJzHfiKnqt1U7p4UKb5Ef4yFrE7PdTLkeK2
RjncIhb6MeevVs8gO6co7Zn8tuUT95U3cOXLhVOWTvaHYeurTXaknICz3IeOoSl8
skiVZko70uJ8pR6asWUlr/zOjlEwZ7RnEUWet97oM0YeA07LDFDkF7eUq//6bfzT
ewr/QfDDsv+erwJBh+9CRHOJyTuDH1WeGxYV8VK3M6VhdTjFxXxFhrQ4pBe5J/UA
17Bd2GM8Urg6VYzVo6x4ajnc1H/ezYLdc459poTffv6Fg2trqFVAj2IrQlAeqjda
lemsa6Np801mUGknq3fjKS13RYGBv/48rCHOT8eRgQKBgQDM5TuS4ANQjOYoOgtF
xoVjbVlndOo+SmdFkZihzQHxcbLY9HXe5HlbLf1IMXz/nERxl+SmYuuJk0EdiM9r
HOCcHRLfBmC7t0GdVvLDHSAX8Ec47LbtKZqyM1U9dn7Z+5q4iywqpaP8pP3+oY57
cgtQax1jle3xhRAj65cl1RBmQQKBgQDVbLqK6wKDfSdZuMZGUtOY0rtamBDCgEU6
rEqBAyCPy5NpF1pomUFcYKWT/wbReFqtuyq2OyiATB0yHHMko46BUtN7qX/m/skt
DHWXVWs1+G4IgEMVokM9jjrkgdY5grrJ68sagKC+bgv35BizHPIqgQuO6qnPSrM9
bevwbQEj1QKBgQCiPE/zeBSnzyjeaTdLxGkR1R+ZX2WqdNdYqnQkiWMkflaSmt5J
4raEj+GhLC5BZsZ6+z480M6XXFWOwSkbMv5WHl824KHvgKcfoh0OiR1EVyjN1gDx
wKOQvjycMhs3FpXn0arjCczS2wGSgPGEpUR4JJhcpfaF6kphZsWDWzVlAQKBgQC2
ivbKltNhj4w2q1m7EGC3F5bzl5jOI1QTKQXYbspM8zwz6KuFR3+l+Wvlt30ncJ9u
dOXFU7gCdBeMotTBA7uBVUxZOtKQyl9bTorNU1wNn1zNnJbETDLi1WH9zCdkrTIC
PtFK67WQ6yMFdWzC1gEy5YjzRjbTe/rukbP5weH1uQKBgQC+WfachEmQ3NcxSjbR
kUxCcida8REewWh4AldU8U0gFcFxF6YwQI8I7ujtnCK2RKTECG9HCyaDXgMwfArV
zf17a9xDJL2LQKrJ9ATeSo34o9zIkpbJL0NCHHocOqYdHU+VO2ZE4Gu8DKk3siVH
XAaJ/RJSEqAIMOgwfGuHOhhto6A7MDkGCisGAQQBkggSCAExKzApBglghkgBZQME
AgIEHJjImYZSlYkp6InjQZ87/Q7f4KyhXaMGDe34oeg=
-----END PRIVATE KEY-----

This secret key was generated using provable prime generation found in [FIPS186-4] using the seed 98c8998652958929e889e3419f3bfd0edfe0aca15da3060dedf8a1e8. This seed is the first 224 bits of the [SHA256] digest of the string draft-lamps-sample-certs-keygen.bob.encrypt.seed.

5.5. PKCS12 Object for Bob

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 5.1, Section 5.2, Section 5.3, Section 5.4, and Section 3.3.

It is locked with the simple three-letter password bob.

```
-----BEGIN PKCS12-----
MIIX6AIBAzCCF7AGCSqGSIb3DQEHAaCCF6EEghedMIIXmTCCBIcGCSqGSIb3DQEH
BqCCBHgwggR0AgEAMIIEbQYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIe/d6
qDQ/28QCAhQGgIIEQJKA5kzRVm9d6rEwC/0RyBSgpPuSROUQTjspt6EhBZlgHc3u
FTCPaO5P/vpeWaCnBRarGFn3DmqA3JT+59bmRpGdiP3Zrlk2EbHi0yrd2P3UFDnX
qRkkI+7pf6eOHWJRntJA+KJS8v3tZ/hpiEKAEav/Mq0IFNFyEiZpCkbKCX5auDb1
p5c3J2MNg/WNBfpGJUHKVIzuIF3H+8LfFgayRsDsppoUMffR+GmdL8nxLiqhraHD
+Iqr3LpEroNi/iZQWUTFTUlaePf/2KMqaHOuy41IVvcH1jIcLXHGNa66S8AP/Hj2
TJPPg/lve76DVaGdEnx4QJd4pBFQac90zmhxU1HZrvzubK9t4e5lr80wpd2djvZK
wSLzUgtQZXq8pSs1r85vrb3KItdYGF6SZpX029FS7rY3uYth5SYVUQWdUYYY3S0/
nsaLg4MCWUO4Sh7nYJZl5Ijkk9LS7JhmwKvizHRRTXbLyRDH06e+jCRgLcU2WSUq
1bEr9Jy0ucK8zNPTf8HWBTS0ubvy4JfO3mVp4REX/8ozXlLztWGblFGbyaJ9Y4ga
LM3JpKxMtb1UTxoAyj3iFwGlGZFGKBlWplr+OdkKkC4dloFE22IINfLdRNLV9mPO
aGZhsDheB8iVOtN01u91BlU68Q7AL1ryXWUSjouKGRSU6uMDLZ7rw0wlZC1m4oLG
BF8CmO4ELmbOci78fBs/qDXlf3BJazcNtciamEsQPYRGkHASBRYtoDfVy6mTT40o
obdrZigcvCwttDBu7RtynAQVZ8DvKzxFGhe2p2Yc9H5A5ML7IwqNtYzheduBAQTE
jAU2jMqwnZN5wULEnH2TF6KAQNrKdtBYMbqkToKgxf5Zf+cJZbyQq7WM6nVfOM7g
kcFdeHDn/CWoSNHI1+JA3wSDM06zkU5HMd2MpT1RLTSaemImUKCAGYieJmwNQxR9
aYHBBw5BNBw1XRB7WRka2Uah0Xq/wAgaI/o9L+mShDRFJjFi+t8AV3KR0WWHg02O
9qchX7P5H3Sy/tq8yUQIol+hRiRjkfi9qy6AxIRttrK4WbW4scUtBZSkg9uFkTVU
ybnV6WvBpn2SrnwF/E1ueKARVmouWJ/7fiLJXk6wVvVtuBZw2gE5QGfuCwq0PQsC
xPx8MhNl1KZYDVCGsyUr/LMHeKNc31S2HLGQK7kh/o+QQazafiJocQ+kRbS1VX1D
nQlIhz4zvKsBgzHpoe3wQcfAY5sp2ubepsZ5T/YHkmroBmvA4g1vi7nlCetgxXrh
2V6OXvaZ+BnfsYxJeUZGnNMNEDFlzS7xB18ojtT5JN0o+9tLsdikdikl69IsVv+2
eCv9Go+wh19cSAL24rkzdKVuiIAXS7tzel3eWGjdKoq3Ke+tfJtobSGrB39xgLVr
3ho63hd+qTUyjcAhVL3hAJinv+/KT0jR8fq+CDsXMnCEWugHhwB+66NOr876MIIE
bwYJKoZIhvcNAQcGoIIEYDCCBFwCAQAwggRVBgkqhkiG9w0BBwEwHAYKKoZIhvcN
AQwBAzAOBAjiGuDSkfG4UwICFLWAggQogyL08hPtUl52dkO+BVimcGXW3FmDrT0D
gU3Drd0P76KzYzd2lLuGb9dx84wx0XnFIXeBM4F3QSDbCK4tOuJ6JRaEeUoCAyZd
XyHtLjVeuozt2xHBDUgQVEO1dZHtk1VUgzLSCha1rXjcwpa4+8xqqoVM3Cl5uBh6
QLUNey8Z3YlKlk018Tdge6OOUrg72BPKppNfJlN4TnOFwMVMA/qHAJl4pL1YDpmc
5BZm4tMg0HvPiz96uwjEhw1GZFGOgZIogeVJuqCNiZPDjCFEDgnCw6sciS5Bi+dX
Km0VUdamSr93e2eEPLbzxZR0E0A3IcOj66iHuZpU9YhKzsAIhLMxT8kF81I0ZZzj
8N+P1hnkjdVWuJLg77pkXxQJyvuT0e2oc9r/DCHjckneen3+E66IKsYbib7sX4g6
2oFBJs+7xQopy69pC8jCn3fx61t7AFx2RIvuVHY/eU4sXoWkJNqQ3Vxj2SPWKjzJ
4IIvWVxIFiQjjOtDFdGYPGukJXn62Lbb8CFgam9s4jDKnr0LHIngVeUIgi4wkvva
QzZTzXfUApezQgQqy4x+ogdiYF1UOa0OaqvrGRiiJlMdRi0/MDy+jzkX5cULhxkF
vdBNCirv+3zBaiJ5Eu6q0zP5Cxi2qXhSbehZqvTPB4dD/vu9yxHpZmUCvzm7H213
Tdrb9WxHOc92ZpBzsfiCA1smVwTDFVGa/kqN6noPw0qWZANIk27/+apsTkBYaVpa
jpfn9eydi5eV2+pEQV08fh4OJfiKbHS0l2E3Gp/rPm9lVgmCmjBWh+Di1k4qgF/f
lsxWgzXNOxPntpohnM6AZDxW9Sk+BElDLYS4WFwUg679BsJG6hQqAZKvG/8agSH2
k+TKKYUbXbFVCB0+iuNZIwgf4qxGzvI5+Iok+OcxuGCqwOu30QbfECEG01QbKETn
ic3kMiZ5Cxt7NQSuyEYAQ/AmvM4qo0x7Tw1r7tR8BcAEF6fGxd2VXIV8Tr/pXGO2
HL+0iIHs+Ob67zlTHr7wUB4tCp9LC3IIWdsr7KcSRNEMXpUIFI0etCjNgCU3iT+R
915215OfWNGxQfaXTEyMVNaT1HpwihIisSb9QHbagaRLbYmqJ+ILSECADYQPEWf+
LTO1tcOhkIb6BiwVWUuOOqNj6ILJM2XvmknATyUj9MYcd77xOJzMrJE5VtaM5BVT
oRpcOLfhYOmihceGSEqXX5golkqfLUze7zlslNWMYTTLw6tC6I+c/IUIWJnZT4m2
RbTQ0krfPn94zbTjrG42HS5+Ke3ySV6Fv8MZ+s93yY1v9iB6cVPEUteLRc+C7e7t
```

```
lw0bQ2+MyAkjenS5Td+3tC7lR42O2CSfY2SaOsRv+EaYjTGzf9F3TM706o5+VZrM
gtIKtw2okRcjRhaKDfhui6jo46YYzWbrgOS3vzc60VcwggNnBgkqhkiG9w0BBwag
ggNYMIIDVAIBADCCA00GCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEDMA4ECEyHXPVs
ncxTAgIUQ4CCAyDSBlYeFnsa4vtKApbLnd9FENDYeYqkKmj0lkDagMqHC22/nQ9v
gz2lOo5FQJoaJx/WSorQt0Jny1QP9vZd2t+bkfoaXOR0MtmFY5SOtYEudJplrCz+
ZEw8JlePJRP0Q3lnwEiSk5NnXLRWNzurIeuyZEd1VbTvi/rF22sRWlmU335L67zj
P1sPeXkBpIYCPLHw8E4rkaC8G1ko5wyrnhuqL4ItzhvOORvgRaDflpP9WTj9LVUv
FD5D59zgb0ptaW0jIw4JplIGXIEZIynW4KfkWy2YJvsXiuLHvN3Z8qL6VtxNGk1s
g340uKkUUlzmtDJqGT9RVkoYBXxN7KYesbSttONhPwdv/MxHrEo8TGHZAvbmwgft
hOUrc/WVtUopPEs4QgrsA8d0MrSd5lVtPW0XPsBPEnLuh7dqAlmgztYlP4Yztk2/
JJ+E4MosmhRjbKzM2N5WuGlDC5m9KF/5JjNVwQ7e8gMeUv/3gizgCG/4Mgng0VGG
IxGzzBoQXPWCKdT3sLQVyt4/pqPBpZYnP09bmkkY/UIa1unNB+WWpLOkKSzD5wRv
/2xmNO2D37DnHwTFYC51ZblKz7FGjOgCwG95VPc8NQ8aG5rqpQ+muq/Jil5mXgNw
IDeM4bawa01UKEzqTGQUb3gsJMGiVOhgtOrBiO9Kx/2PJolUuwZGcbo4oGSVR7KH
lLgIuC8aIQDyFURVYRCNwOw5U7JN5arkvZ4ty0/qk5UbjxQuDkF8o6ZdViO3l0Do
C+6zvncDx4HvUd6uQ+u/kZfr8qfwM5o6D2qXhS/ZHSkq2xwIzb47uUUqaeg3yOZJ
++na7gC+ibtHXXnNsHUvPbpCn9qViFhzilcQZYq0tZxDKa0E/pzEP/IA4IG24wEL
GnyuUIHXBS9T0MchTxl7BglycOPRDnFKzMQfUXY1rAErK76cs3y4VQDbfYDiOzsa
1qqMApIX4i/qKFdRvDuLxtZQbVA/rNumm40LPUQ5OvEngIESA74G+//YQbVjbMjP
y+hm7/15q5LRo9YxCS49KGlz4NG1QMWjnfkpOCNVZVpaQ7TPGOIYzBL6kTCCBZgG
CSqGSIb3DQEHAaCCBYkEggWFMIIFgTCCBX0GCyqGSIb3DQEMCgECoIIFLjCCBSow
HAYKKoZIhvcNAQwBAzAOBAiO/0ICbTbZLQICFOwEggUIFwT/JI8UjJQPfYTFonJE
o8zEbpYWXKboqw6/zZsMGmAnUPgQNQDxyuLVprs5jUc437kVB2M3F0x8DjmEppeb
tHfIoyjoXF7jdnA4EF38tsso0K1nMPmSgl02iYZtOqsOvBpfeO5Hj4Ovhi26J9Pz
TwPcgl3QQPqfWv7CwgGVn4/hntBAriPSE4gAlfAcqkxtJBm01QwDoAdsOKOMsYnt
gWajpr1J3Hm+34NPL04Usf1OpcesPUJ4CBxNyLXxjjsOzD78WVvKY+N+j89xTsyt
z5Y0fEkFqrcl8pgBQxH72jBwSCm5YwHz3BhWQgr2bpWJ1f2LWcVsnrN9tx6RhQtA
AkcyNgX/ksp5EW4JTo+o6oXLRhXIYauRrUrisMY++b8ZJTp6C1t0RW2QdqgMZghS
ZgaW6FSC6Dy2Dd/ezdkYUCgiEtq8eSxF/8WDw6Va2iGVSNt4/p/OJ97yN5yOJ0K1
g0hATebU+I3E74PQ9RK84FfJvyHDBC6fvYZW/ouMcgp3YmAF+dTm74Hq88X4daV+
/UPYf/cVpyiwcBTg6H3jrkrs0yKoWLIfrIvMNBeeKZ+fl2Enw1MFzkLI4VGD/UeR
wrbhN0SHkh5lIGtu0yRTfq6msYQpkw+jr7QwJIdQyrAoaaVaRotVyvgTOLlHw8r6
o7v36yoNov3kDPW7DfbSVTWX5lIyQn8NqMwa4N1clWT8ukfZXSaYykFSqF3w5zal
a4iIhu03GjDcfiWLMUlYVAUcvSmcIULE1oW7FKiJc8OadeIu0JBySRSEvf7B3w8l
eYUs+u/h1ptrZZKhe1JdAtlszvHJ0DD0kMqA6Ig4yomscGSol/sRUqpecIQwVZTC
RRq9dJOFJkKhKD5Eo9E0Z2snp01fpUF5qlMeBjpYgkX7jhyFyvq+qDqBAY8izvkc
ruE69WooBVyorqKHURjWtY+rhzcB4+HL72wZKzLnY3iUjJ1UANxM8mC9fpD1NJt/
7epqzPyZ2Kd4GJVYi8sQpFKf4tRHDr0tI5iUB78qj1EBp1w4qvRn/jC4ii7+Bas8
mz/AJ25QeviC44Vj+eT2YYXafDivrmoeBuVMIBbD066YnuBC2CeKydNWdiARzc3I
fhcuhVwq7riotYfyDqd4e0Jy7Y57pbwv4Qwz1yCxRjSwiFQ7/fRa2Cx8xtxKcC/A
4LGnXAKISy+uNbDWA7AYaP6RmGgMCaNiXy3F1zvxnE3bv68tXRF9vjuEChUq56N6
992qhoBuHP0J/mRItw+JoI4m/OFnEUGT3bNyxpEFyA7aXBE91aQdSXl4a97nC0/R
SFH/fRwPFYgxr3XdCIf3Cw5PDs25YNsXWCsDCVejWMFrwOzmDwa8sBkY270+rGv7
6qXvb/uGD3M2C+DySVy55Zd42wjghSezgY6taT0tqKfLOS6Vl4ELU78Q6va2o8Ml
cUdi343tOi60MZgCDUwPP8TjKZINh8u1KNhzgpwNLz1gE0dd200l3bbzdZ6uio3R
52WQWRCk17Z9lUesCJavytcAi0mMefMxBPMOdnUi6O8TPDRA0mcohbE5rybwDXAo
B/VUbwgM0/qCpZ7VcSKN1lUuoe9+Kho0NK/gyMEvntMxGNNI8arV8UkeFollPhrt
umvdwqbVCeN8TBj5vXo6Hu+eKB7AVwjBk/rRHpZxnnVGXbm8HzM+kjib2cY1dius
```

VRJ/1+Q9GXuo135tQbobgcMzAmqAqZp9kDE8MBUGCSqGSIb3DQEJFDEIHgYAYgBv
AGIwIwYJKoZIhvcNAQkVMRYEFEqzrDFTAkmcTeNueeAlYZU+iGIlMIIFkAYJKoZI
hvcNAQcBoIIFgQSCBX0wggV5MIIFdQYLKoZIhvcNAQwKAQKgggUmMIIFIjAcBgoq
hkiG9w0BDAEDMA4ECCNi2K1bMEiBAgIUdgSCBQDLIXo4ExcyE8+4aiZIj/Wnh/SV
VVR0n7s4PGCbXt+VrOHd9YzTuUicAqIcHH62dv7NSy+fgqZG7SmVR1IodadFe+5u
sAzXoyyhhEe2c+ToeVbr5rs+vBvQUyh6X5XTV5QVOAkwSyKGjyfdy86x1Q8cL2D2
BM+Rpkm1cFtjgWcB46U6S6w50sG7XOKSCMI4a6rnHPVgPPdXMrj3VSPJY8bhBqED
PVTnfSHf/wKZrIi54O3F33B5jt6Cm9+9m9Fed8n+81w59rRom72CY9Xii/ULER9T
HwjxOZOQ+dIml23KauwexuOGjii0UR8MeM/A0n7UNys+bZTulgdpWW/mDhJ+eLAT
nhJw5ro/AWa6YVXG+t5k9LjdJ1ZmqS4bJxvBwilpEGoh0MM6Yp0dr1XM4mT/E0JM
WD458Ngs05CuCpwAUXGdQmgrVsFrrV0HTyHeVLDhe43J3GI6HCWJVOeDQzzmaO3A
M+IooRDkTHnJMaxUXphKTag5+f/smNYEhzVjZeIc8GFZ36eSI4BNGHSXFACwLu2T
hkzpXMmg50JAUhBYxqE/fVevLUH4JPLgz869wk8gRlUBo6ihQGrnsx7ZO5IsYahE
Yjz0N05PVPJYMLSyMovG9i+LpzQ49gIBzPu2fdLR41u5n5O5mG1Y4aJ7OCJxMORY
hWHuctHdGdpJsgiq8+1iiUwmfyCfb0ZL3ePMU+W0zkAsyn22aK8jDBLLVZlvOZIV
qR3Gx4QFPSk6qCMQ0E58VkMUMxYvClzTwSeEMu66eND/AKTE+XXV/d9bmSmWGk7Y
8XrDKLKfmRdrlIeondVJv5mk12YKxBPQGeUqK5XJUa2dzH9zvfEX8iYzdt4281QC
iXJ3qwmbT+8RoOLBt4KyOs2e2ZSZnjrL9OO4oUsHIOyEfjwnWoLhKbkmun8GJxoB
2yCzTawVQf9/qIUXaSzcp23AV6Lf1k9Of79HYPW3cQJAtjf6XBVE1xVZPkfTuC3y
VLufljs2ed/ctpHg9nuId/xHFH7t4HbmU3/ZufE1GHnsRQ3kbnqA5WXerd9UzeoD
aVDjFXGrITp8env08GXYvwWGXLL150l0DuJSv1E+1yww86SNjBYUTx0r0CJjjTk2
7vIUhAYUEA+J71IeifqqPDKYXnrCdUEajbfEdek30WiLR+ChEvEp48Mla6UVTLm/
mjziwbsxm5QlGccmz13e32RiyrfseB+RyllmzeJtydP2IHkWK7pww9yOlPK0QtZs
66IGZKqeXrWBk9QFYDX42gAy/xTfglco4KO7akhp3UzTIQyTXnt+OsOScc+ArVm/
dwClm+ZxybtOcVyadjpKWydyfAr3aTkGxX6RmHrEWr1R9BnMGPYesDs+yeVNs1Qd
Dhff/bQLwCLXdGLWwLe6kitUiyi8F3bdfPjR7R61lEUvJrBm7YLmgdxRCJ02LFLG
n09iSMNe5vmiNaKiuzfb4Dp9dqEMhmJfdsTURagfJIyqULoe08EIIozahivbzoWV
A6oPAkk2D8DnTiMegX4IZ/Zb3LPxJKAeXO3Ys1YQrNSNZ3B2ZISBapzGzhFZfRVz
POmXhN53pDhlxkw0btkKblYA9CvP+kzgwekzCy/Mlq/HbO38CV1NKzay3yg4nteh
J+v9/k7gaqKmo3ZWMGk0WGBv/GFxYhmeNd14Y65D9TlypM/zrXSyGoOqZgSA6HlA
gogzwwSaGwx9n/o6czE8MBUGCSqGSIb3DQEJFDEIHgYAYgBvAGIwIwYJKoZIhvcN
AQkVMRYEFBfFhHvQp+92kDi4s28IvJK1niuUMC8wHzAHBgUrDgMCGgQUgwafFeGU
n9Q1rAOUCgw+KWxk+8EECJ1vqXe6ro0FAgIoAA==
-----END PKCS12-----

6. Example Ed25519 Certification Authority

The example Ed25519 Certification Authority has the following information:

* Name: Sample LAMPS Ed25519 Certification Authority

6.1. Ed25519 Certification Authority Root Certificate

This certificate is used to verify certificates issued by the example Ed25519 Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIIBtzCCAWmgAwIBAgITH59R65FuWGNFHoyc0N3iWesrXzAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjBZMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzE1MDMGA1UEAxMsU2FtcGxlIExBTVBTIEVkMjU1MTkgQ2VydGlm
aWNhdGlvbiBBdXRob3JpdHkwKjAFBgMrZXADIQCEgUZ9yI/rkX/82DihqzVIZQZ+
RKE3URyp+eN2TxJDBKNCMEAwDwYDVR0TAQH/BAUwAwEB/zAOBgNVHQ8BAf8EBAMC
AQYwHQYDVR0OBBYEFGuilX26FJvkLQTRB6TRguQua4y1MAUGAytlcANBAFAJrlWo
QjzwT0ph7rXe023x3GaLPMXMwQI2Of+apkdG2mH9ID6PE1bu3gRRqIH5w2tyS+xF
Jw0ouxcJyAyXEQ4=
-----END CERTIFICATE-----
```

6.2. Ed25519 Certification Authority Secret Key

This secret key material is used by the example Ed25519 Certification Authority to issue new certificates.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEIAt889xRDvxNT8ak53T7tzKuSn6CQDe8fIdjrCiSFRcp
-----END PRIVATE KEY-----
```

This secret key is the [SHA256] digest of the ASCII string draft-lamps-sample-certs-keygen.ca.25519.seed.

6.3. Ed25519 Certification Authority Cross-signed Certificate

If an e-mail client only trusts the RSA Certification Authority Root Certificate found in Section 3.1, they can use this intermediate CA certificate to verify any end entity certificate issued by the example Ed25519 Certification Authority.

```
-----BEGIN CERTIFICATE-----
MIICvzCCAaegAwIBAgITR49T5oAgYhF5+eBYQ3ZBZIMuujANBgkqhkiG9w0BAQsF
ADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMo
U2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0yMDEy
MTUyMTM1NDRaGA8yMDUyMDkyNzA2NTQxOFowWTENMAsGA1UEChMESUVURjERMA8G
A1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBMQU1QUyBFZDI1NTE5IENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCowBQYDK2VwAyEAhIFGfciP65F//Ng4oas1
SGUGfkShN1Ecqfnjdk8SQwSjfDB6MA8GA1UdEwEB/wQFMAMBAf8wFwYDVR0gBBAw
DjAMBgpghkgBZQMCATACMA4GA1UdDwEB/wQEAwIBBjAdBgNVHQ4EFgQUa6KVfboU
m+QtBNEHpNGC5C5rjLUwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29Fkw
DQYJKoZIhvcNAQELBQADggEBAGV0x0OEzgYlRKixMcztiikxxJDbmRat1pcipD15
1n8kiBoGhsT4fNZJVoL0OQBa/WTMntL+qcAk2itqZCNIeZeGklUljXBAz5tkDRAF
f/v99LEcsZTcuIbnJqz35danQkp4/upG4hPkfx+nbc1bsVylrITwIGOpnGhz7z3m
VCk03DFE3Qt4w9mlv9yuMse33nmsBGXog/XZvM2JRY0iKt0xksQqQD9uYm7MoMeH
qQs3Ot7EaoPj54xyWvy42run6TLUye64D94SNjB/q/wjL96bsVIKGrRn10T1ybCh
4F5HD00hQZgP15Dlb1rg+vskN8MSk5nuD+6z1VsugioW0+k=
-----END CERTIFICATE-----
```

7. Carlos's Sample Certificates

Carlos has the following information:

* Name: Carlos Turing

* E-mail Address: carlos@smime.example

7.1. Carlos's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Carlos.

```
-----BEGIN CERTIFICATE-----
MIICBzCCAbmgAwIBAgITP14fVCTRtAFDeA9zwYoXhR52ljAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA6MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEWMBQGA1UEAxMNQ2FybG9zIFR1cmluZzAqMAUGAytlcAMhAMLO
gDIs3mHITYRNYO+RnOedrq5/HuQHXSPyAKaS98ito4GwMIGtMAwGA1UdEwEB/wQC
MAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB8GA1UdEQQYMBaBFGNhcmxvc0Bz
bWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUZIXjO5wdWs3mC7oafwi+xJzMhD8wHwYDVR0jBBgwFoAUa6KV
fboUm+QtBNEHpNGC5C5rjLUwBQYDK2VwA0EAwVGQWbdy6FQIpTFsaWvG2/US2fnS
6B+BzgCrkGQKWX1WgkTj4MEOqL+0cFXLr7ZQ2DQUo2iXyTAu58BR6btcCQ==
-----END CERTIFICATE-----
```

7.2. Carlos's Signing Private Key Material

This private key material is used by Carlos to create signatures.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEILvvxL741LfX+Ep3Iyye3Cjr4JmONIVYhZPM4M9N1IHY
-----END PRIVATE KEY-----
```

This secret key is the [SHA256] digest of the ASCII string draft-lamps-sample-certs-keygen.carlos.sign.25519.seed.

7.3. Carlos's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Carlos. It contains an SMIMECapabilities extension to indicate that Carlos's MUA expects ECDH with HKDF using SHA-256; uses AES-128 key wrap, as indicated in [RFC8418].

```
-----BEGIN CERTIFICATE-----
MIICNDCCAeagAwIBAgITfz0Bv+b1OMAT79aCh3arViNvhDAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA6MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEWMBQGA1UEAxMNQ2FybG9zIFR1cmluZzAqMAUGAytlbgMhAC5o
MczTIMiddTUYTc/WymEqXw8hZm1QbIz2xX2gFDx0o4HdMIHaMCsGCSqGSIb3DQEJ
DwQeMBwwGgYLKoZIhvcNAQkQAxMwCwYJYIZIAWUDBAEFMAwGA1UdEwEB/wQCMAAw
FwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB8GA1UdEQQYMBaBFGNhcmxvc0BzbWlt
ZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIDCDAd
BgNVHQ4EFgQUgSmg+iOgSyCMDXgA3u3aFss0JbkwHwYDVR0jBBgwFoAUa6KVfboU
m+QtBNEHpNGC5C5rjLUwBQYDK2VwA0EAzss75UzFuADPfd4hQdo5jyAQ3GvkyyvI
BdBGnWtJ1eT1WuMaIMhi1rH4vPGPd9scwW+sqd9fG+pv3MShl+zKAQ==
-----END CERTIFICATE-----
```

7.4. Carlos's Decryption Private Key Material

This private key material is used by Carlos to decrypt messages.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIIH5782H/otrhLy9Dtvzt79ffsvpcVXgdUczTdUvSQsK
-----END PRIVATE KEY-----
```

This secret key is the [SHA256] digest of the ASCII string draft-lamps-sample-certs-keygen.carlos.encrypt.25519.seed.

7.5. PKCS12 Object for Carlos

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 7.1, Section 7.2, Section 7.3, Section 7.4, and Section 6.3.

It is locked with the simple five-letter password carlos.


```
-----BEGIN PKCS12-----
MIIKzgIBAzCCCpYGCSqGSIb3DQEHAaCCCocEggqDMIIKfzCCAvcGCSqGSIb3DQEH
BqCCAugwggLkAgEAMIIC3QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIwS3R
pT1mkyMCAhS7gIICsGKkBm0nci9VHfqxOTWy/lkKyQeF5bwsF/9gZrqUym1KtHZF
a4rSJIPUctmzqVnhGmfW9m+LEi7Em9rRmUIQbDZt4kQDG5eDk7AdhyDnB3uZDG1W
4cAeUVXJMzGfnwtzy5TzBZzEo5nnVX74Al+PDW9wdpbv2TIriL0m29fBT+7HVS9F
Z/95XokSwbb6mmCYeGiPpNEaoeUeuU4zrh/k+JJqDuqNsU66I30wH0CFmk3aarBV
3LkEeCjKFkngzMOZqiKZu8D2hEUjsGQ9ALsRn7P+hIWNFIgjvqgcCMTF8fLK1C/8
vYGD+HOpnn23nLele4b/qpFYx5kJ0bOK1Zo1SpgUQ7Bu6gectUceyOgi7CjRScuV
ew7918ZY0ugyYoIWAT0kecPM0TFtxAn19JPXo4jBYAlwUtx7GYAlDkgZCb/0dbkv
4L+PAeJK4kVDREDQ6ch/6/hlqU8xHeNzdagEWYL6FxWDiHebASxIvZzqkLd7RV9m
dL1FXst9R9G74jOs0WMMFmd9toyOhD0q6Gl9catOrolCVS/CKaC0CucsJfiKrlJ/
duQkt/JwcELveuOg60u2uaGKUqHmFhd3+6omk+wNBoY+0D5MmBZ/xnrVELGmzp94
q0f/HfZPT6sxkYBGuP2eUA/qr/zimNG3TuGVch/MdnduuVhvAYLyh1gbA8yRm+I/
zGCVuAqhsHITTx7Fqc3tyVp/mLYUO0QuwmgAw6NhzwKZf5N+tR0DZGcgw8rZpeJA
yTxVFcjzXvoShxog7RroR9Nc4FwJhWI4BO241OHFEiQZeRk8vzI8WIFXnn6t42/q
j1mV7Ba42zxPEGoY3mObKwjR6rDp6KwmmfkghpwMPU3qP2/ASV8WT1+9GIYHc5Am
9CmSOTiQMluW70Ra2k5ZMlwnbKNyMRbjUB/yHwwwggKvBgkqhkiG9w0BBwagggKg
MIICnAIBADCCApUGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEDMA4ECOMzXMste/8a
AgIUlICCAmgXa+q2JhTLvWsj5SKLdMninTk5uB6HhOsDKYR9GDg/cABqUFxycROG
JeJuewIRkJhsfdXJi+TSRtnQOqpyVM9oRUdxcbGuCI98fEbLmVyr7KF8GudTgC+b
eaLjn6HYkWpv7lWdvsFG8BEy6Jqi3/tP9PgNvpCYgVVM7yx6SX8QArcLSQkxbTsv
Ae0iN18H89W9xOHEz4Z2qHYyb7f0pPHrmpTGC6qmtvo1gNRsKTF0wYeQ5Sy/9U3f
oM6bIcrOvHDksaco4+5n0zeySDETY8W4mO1K0uC/t0oTOScYGBeRhVr0DQapZGT/
Ej5LpgjXOuosAoT3IKnMwK3C0OZ8oBzcvgSpeAa/V/OTKDpZb22yq6sEaHAPoUqb
cKRJmB6HC5mdLs3n0uP1vlZuYsHu7Evt0Uhns9pbklJDiCgM+4SFgKTRbd6Xt8bf
GHkWnmpv4pQL7jjzA3epP2DHyC8MJaDvleWY7Z3t/IEtkzVxflLo8kT21edz12cm
uFVK9ilMW3eJuyiRyFXFPgVsuNi/HFnijXFgxzAncP7fFP5MCsOo6daiEjJjemKf
J3D+HdD60gFih/eX9V+tGl4y7/jtxCRA/54mit4sCy3LC0++lEp9AtFwGYrDw825
uGj27a7mE26qgGdGXdzT9UJ8FfUsIoRPrG38Q4mhS10pTarNucWOGjkftZiKJLay
rfMRf3HYxOI/7iupfxYLK/4/FODijaHzAfSdQf2Bo7csPaz2HQkK/0nyO+tt68S9
pUCjEfV6Liy22tang/jXxPFbBDK/P68MnmgR8C3PcYhPJCo/K0JR2/8F8pVVEqd5
MIIDPwYJKoZIhvcNAQcGoIIDMDCCAywCAQAwggMlBgkqhkiG9w0BBwEwHAYKKoZI
hvcNAQwBAzAOBAho9g0tQyYTvwICFIGAggL43SpNCoshZX3ikmK1mOIJpS2Ah8Xv
94S/5NA8kwHtaNXpLrjYr3CyRL93USm55uvGAtECR/EblON9zeo2p0gK2JPSbDr6
/1oovo7UoZNRoRBZ8pUegVWJswNWjqvzVu5JIRmpD05XjVDKHbFqiXAqtj9/w3q0
Qq/p/M9UrLWD93hyLNdIppWr2KR2it9mASTKEHX9dqXcTOG0Kp2GmrfGNteGL02j
qVKZaZyYI8gkSxhVLS9zzgf1OynAkzYQsoo+GKhdAW1fJECemAyPc3L+eeARw/SY
q1d5QVwxKfYpIJ2wiiavdeRVNbWiwV7Ti+P9PtPx/hV22NNLwMhvnJcHaSS1PaOi
SjoxFJ1EJWGEs0QwcdwM8iN3oVuqT5HU/edMgx9TLNTiE1g2GEq59I/RwBtCL8Dh
```

```
OzKnUb4PU1Z81+HimV3KPI8g3cduhYaBR4HfqAhMnc+w5HXI6J3C1NtAE/izZ1Y2
Od7l+GTJfjPgzIy0hjqfbMt8uU9D9aPr2XjNOWoKRSojae16v8bLx+dFn6RMxFUS
g3nLEZ6EDpyrJfpGPm6mPgZKSXtvnHuFcbS+utkRuVAtqu07r2XpkGBIJLNVIRHU
5gLACbTj9TPcAce6RLoaYSDgOuFK0YZMdwzhsAI0YMpyHsUEZpQ5tjWSBY6ENbvF
7+QhmDnf6N3Bj+vxUtGS40pVsYCGbmOD7UM5QpUxIgVkpPrfRokOZs/fi9sW+Xy6
eQ2Brbn3t9C2TAsORYzFbuBwuTCqFW/rXHS6iffJpx2eAg3DCqaUAJjptSV/yzj4
vxiXlDB3fMRcpNd5Je7DoHS4axuj7SLHdpNoUHs+qQsG6yDM5BEuXWGxo/L9sGhe
XQrUnkZ4m4g01sfgTOfDNurXx/oP0ym+B50q6nLUWv0tYZpmCVil358dIEGPPSMY
AMXh05tIPFdYSJ3WLs0cxy5X4sXZl5w16Pzeb9SF5topqRUb5PDTfVr2bQUMwTbp
99FcOQf6cg8HXyT+8b4qKp9WyjCBxAYJKoZIhvcNAQcBoIG2BIGzMIGwMIGtBgsq
hkiG9w0BDAoBAqBaMFgwHAYKKoZIhvcNAQwBAzAOBAgNhfODEdzSrQICFF0EOCEq
Fie1peicS9OSXNQjLwbN3kO8lYM2HqeSZoEKJ4JSFlV1kWW3xwfu5aZKrGEYBfGM
d8renRijMUIwGwYJKoZIhvcNAQkUMQ4eDABjAGEAcgBsAG8AczAjBgkqhkiG9w0B
CRUxFgQUgSmg+iOgSyCMDXgA3u3aFss0JbkwgcQGCSqGSIb3DQEHAaCBtgSBszCB
sDCBrQYLKoZIhvcNAQwKAQKgWjBYMBwGCiqGSIb3DQEMAQMwDgQINFcqIEMfd9UC
AhS1BDgZruEsSaBY+Cm9WKR8HhH3JXh+AoMSrwkDCKytWt+MNIXB0jY2QZHDbN3u
Fn7qHw06MDthnKniazFCMBsGCSqGSIb3DQEJFDEOHgwAYwBhAHIAbABvAHMwIwYJ
KoZIhvcNAQkVMRYEFGSF4zucHVrN5gu6Gn8IvsSczIQ/MC8wHzAHBgUrDgMCGgQU
8nOYIWrnJVXEur957K5cCV3jx5cECJDjaZkfy4FnAgIoAA==
-----END PKCS12-----
```

8. Dana's Sample Certificates

Dana has the following information:

* Name: Dana Hopper

* E-mail Address: dna@smime.example

8.1. Dana's Signature Verification End-Entity Certificate

This certificate is used for verification of signatures made by Dana.

```
-----BEGIN CERTIFICATE-----
MIICAzCCAbWgAwIBAgITaWZI+hVtn8pQZviAmPmBXzWfnjAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA4MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEUMBIGA1UEAxMLRGFuYSBIb3BwZXIwKjAFBgMrZXADIQCy2h3h
hkaKDY67PuCuNLnnrQiHdSWYpPlgFsOif85vrqOBrjCBqzAMBgNVHRMBAf8EAjAA
MBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAdBgNVHREEFjAUgRJkYW5hQHNtaW1l
LmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0G
A1UdDgQWBBRIA4bBabh4ba7e88wGsDOsVzLdljAfBgNVHSMEGDAWgBRropV9uhSb
5C0E0Qek0YLkLmuMtTAFBgMrZXADQQDpORBZitzXGYUjxnoKVLIcWL5xner97it5
VKxEf8E7AeAp96POPEu//2jXnh4qAT40ymW0wrqxU1NT8WW/dSgC
-----END CERTIFICATE-----
```

8.2. Dana's Signing Private Key Material

This private key material is used by Dana to create signatures.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEINZ8GPfmQh2AMp+uNIsZMbzvyTOltwvEt13usjnUaW4N
-----END PRIVATE KEY-----
```

This secret key is the [SHA256] digest of the ASCII string draft-lamps-sample-certs-keygen.dana.sign.25519.seed.

8.3. Dana's Encryption End-Entity Certificate

This certificate is used to encrypt messages to Dana. It contains an SMIMECapabilities extension to indicate that Dana's MUA expects ECDH with HKDF using SHA-256; uses AES-128 key wrap, as indicated in [RFC8418].

```
-----BEGIN CERTIFICATE-----
MIICMDCCAeKgAwIBAgITDksKNqnvupyaO2gkjlIdwN7zpzAFBgMrZXAwWTENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxNTAzBgNVBAMTLFNhbXBsZSBM
QU1QUyBFZDI1NTE5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTIwMTIxNTIx
MzU0NFoYDzIwNTIxMjE1MjEzNTQ0WjA4MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEUMBIGA1UEAxMLRGFuYSBIb3BwZXIwKjAFBgMrZW4DIQDgMaI2
AWkU9LG8CvaRHgDSEY9d72Y8ENZeMwibPugkVKOB2zCB2DArBgkqhkiG9w0BCQ8E
HjAcMBoGCyqGSIb3DQEJEAMTMAsGCWCGSAFlAwQBBTAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKYIZIAWUDAgEwATAdBgNVHREEFjAUgRJkYW5hQHNtaW1lLmV4
YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgMIMB0GA1Ud
DgQWBBSd303UBe+a7GCGvCdtBOnOWtyPpDAfBgNVHSMEGDAWgBRropV9uhSb5C0E
0Qek0YLkLmuMtTAFBgMrZXADQQD6f7DCCxXzpnY3BwmrIuf/SNQSf//Otri7USkd
9GF+VthGS+9KJ4HTBCh0ZGuHIU9EgnfgdSL1UR3WUkL7tv8A
-----END CERTIFICATE-----
```

8.4. Dana's Decryption Private Key Material

This private key material is used by Dana to decrypt messages.

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIGxZt8L7lY48OEq4gs/smQ4weDhRNMlYHG21StivPfz3
-----END PRIVATE KEY-----
```

This seed is the [SHA256] digest of the ASCII string draft-lamps-sample-certs-keygen.dana.encrypt.25519.seed.

8.5. PKCS12 Object for Dana

This PKCS12 ([RFC7292]) object contains the same information as presented in Section 8.1, Section 8.2, Section 8.3, Section 8.4, and Section 6.3.

It is locked with the simple four-letter password dana.

-----BEGIN PKCS12-----
MIIKtgIBAzCCCn4GCSqGSIb3DQEHAaCCCm8EggprMIIKZzCCAu8GCSqGSIb3DQEH
BqCCAuAwggLcAgEAMIIC1QYJKoZIhvcNAQcBMBwGCiqGSIb3DQEMAQMwDgQIZNqH
TA2APx0CAhQXgIICqK+HFHF6dF5qwlWM6MRCXw11VKrcYBff65iLABPyGvWENnVM
TTPpDLqbGm6Yd2eLntPZvJoVe5Sf2+DW4q3BZ9aKuEdneBBk8mDJ6/Lq1+wFxY5k
WaBHTA6LNml/NkM3za/fr4abKFQnu6DZgZDGbZh2BsgCMmO9TeHgZyepsh3WP4ZO
aYDvSD0LiEzerDPlOBgjYahcNLjv/Dn/dFxtOO3or010TTUoQCqeHJOoq3hJtSI+
8n0iXk6gtf1/ROj6JRt/3Aqz/mLMIhuxIg/5K1wxY9AwFT4oyflapNJozGg9qwGi
PWVtEy3QDNvAs3bDfiNQqAfJOEHv2z3Ran7sYuz3vE0FnPfA81oWbazlydjB0P/B
OQ+s6VLbsAosnZq9jv2ZVrCDaDAl/g7oD7fY8qmaC6O2q5/Z3KusfMt+r9En2v81
H2vjgrpxnDIXjYuLZdrnNE/slRtqadOGR/WQ358RG+yUmRUbHYHGnkjn9fOGLasI
ZUV0aowivcWyF/kR7QV3VVexgqJMX6k1vzSXRoJ/tnA+1/WPWy1mCJeljGOgYqSV
txtVB61Qmc2XP48F7wyaQZvdAU9zfe11/tHAaKKJWBpE1lIuAEkGtIP6ozYJBFjH
I11tBA8fijTnug+S4OvSgjtsRV/+kSEiW4F+pwE8RuTYfUu7q+Ew0LYdLgkH5OyE
sn0b62UFpR/E1D9exWzohrFbIdUCbjtssXucruAqPNhW/abT0zicWu5nvf+Pniow
2VxvhwoGt5jZ+lkaR5Z+1/GpbMgq47EUyGCgKv+5GAcJxUxINZqLbACJ/MhLfYPB
eJrXz8f5Cigm1wZLisYCqnuc8cGCXjNqNkUlqtzodM8xv4gcgT/zILxmJTZP2q4n
YA4yBQx5/n2G2dZC+pf3kAfbXcp0MIICpwYJKoZIhvcNAQcGoIICmDCCApQCAQAw
ggKNBgkqhkiG9w0BBwEwHAYKKoZIhvcNAQwBAzAOBAjxuoiaSZDbnwICFH+AggJg
k2hcNYtO0+15uLqXdiNhr5Q0JkYcrHdo0wR6G5AgLmwI+TYi+P8EZUjDIJ4TJ3b4
6xv7+3pT8cbEFf6PXcfS8/sCfM7FaV3SpLACLZbBJV52OKE0CAgALZOLuIz5mGVU
tWI2h1x587KeIv5GRPIxumDebT3Gmkkp9Qoi55hjTgn68olSgDaJF8o5wnfODhkS
o110a3x9OwkJSN1AXfmBfj33KnT8Dc4bTfAZy1S5o1zCtaEqnct2Urb4PeO3LfHB
ErBsvY8HE4D7qh6P5ftXHQHAx/b3hbU8jQP1tR0N9Oh0SiLi//ebCeGXWQRdVjL5
+VQrhlQF5d4Kz9Zx79oC36g7C2BxCQomur/F9TT12NPzPpaEGGo6ljB6myAHnYw9
rCxbSxBvbtEtlgJnxxb1Y5Q4ukgyjzK6431Bwq2+iNL0vGc9o2c5ELUPU9zGeLBZ
tXWvdX27aOHjusPfDZl70C5zHiYs1FU6Tkn9Aotc424Q3d2IRTTcYnnjs1VSi1Sr
4bRyB8zBAQmdQrniBW++7eJm3m/EOU0Yy0noUT169m8KNJrmSspMvKS6pyiYHR4I
BvAIkRIjvdtQvJdQJ+Uyr+HH5daE6golW1917b2bXj/41mvXYkJY6W8x0km1RYhH
QJZphWlvNcrHKo46Unk48Qc/5J5tI+6UDTXFr//V34vcpQ2ktp0MAKl1rBH549ef
CsGQTGoq8XHPhksehEEMRmOJDeKTVkKx8xNhbwb395yFCIxfF2NHeDLXP+JyW+nH
Iy2fnBDlyTiPF7YXyGiPjPAgK8LS8GUE+Zq2rWqrGNkwggM/BgkqhkiG9w0BBwag
ggMwMIIDLAIBADCCAyUGCSqGSIb3DQEHATAcBgoqhkiG9w0BDAEDMA4ECOfJ/s3Y
f5bgAgIUnYCCAvi4NaYP4lpAtuXtE02Zqgl9aLFwsj9B/rikBo6O1ZR/lsryJ4PJ
VGYy6NyBPjG67glJVMYiI3Hge+j66FXKXD/AaiMVD21ZmfrH935Sl4ZUKS9tpTJL
QDw3ejpDEDqJUFJZJ/ybgpRAKoNjhcE3B7F7+WMI8Pr70M1Fbw7ytUCAjOf18sIW
prUA8f8O9dLiGgiWyjE5HMzSXEib5IMRpq5x4Q28pBrT8rVYgoQSSyVkfHtU7LDi
Bm68RfBgEl7jIqLdrt2kKxHC3/lC4xXQgFNXeQO56aRp8Yu4VpoRwraVLUO3tJk+
pf1zFfmUei/JtiFlC6uf0PvC2B5h6kAZocE1lLxGIDFH7fTd6dzP7qTDbUQ+uEk3
qsgktT2pcoVnxTanvQmTCEZM9ZKCX5/z7Gkm+z83lGLDDU9oNyRSrxHrRBIvgH4w

3aGH1v6kfYOWwwwaghQOQIZFyzGVRKXsP7AslL+n4ti831TxqSUZX2qy9LpI4Tjp
5A/NLMKo3uqmHFlTLnnYUqoppe88FNY8T/LXnHp0KTkuXFmdKJtp1/ydqh18jBk7
nfLcQFdf1R/5okysblRtaMujlhelymT7MoM8u5C8ceIO7uWX8NI5B/IB+Yn2BvzZ
9LXoSia/wHjTu7UK610o7WOq9qTYe1i1x+HsmJaOC6hpaQh6b33VWDrHJbl7c/4Z
tvQ9qAzqkqIhFWMRXNK+32jFVAgXrD8U1QHW2ip5s7W/Xtm1AegrhG1nSQgJezYl
OnE/t2PDWuPeW94kR0uv1fNsh6plLyZYf/BaqhoGCHsa/ipD86viVSZDgJ8ASVLF
eLUK3HYFMhJ+MLEzZJffYZAOnbYoyNPNc0vc7dpbk+ZMnlb5bDFcMCpm7+fWOjsC
nsNNL9nqQlNHHCJRKGuxO5rujftbPM7R3GLT9d/u5e9YY5cX0RiDLxomFffIj2Yh
uRoyX+8WzESt98I/KmAraWKXnxOP1FEWajtNCrnGCezDKO3xEHTQhECpg+z7O4mj
MjN6MIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSIb3DQEMCgECoFowWDAc
BgoqhkiG9w0BDAEDMA4ECL2Bz1vW+YZkAgIUugQ4YOyEjke53NDvCFR0ciUHZ7re
f9/wPx5TgV3qzGhfR4bP2rdpiOt9hAHVK5cmUAR7+wjAJiYdLUQxPjAXBgkqhkiG
9w0BCRQxCh4IAGQAYQBuAGEwIwYJKoZIhvcNAQkVMRYEFJ3fTdQF75rsYIa8J20E
6c5a3I+kMIHABgkqhkiG9w0BBwGggbIEga8wgawwgakGCyqGSIb3DQEMCgECoFow
WDAcBgoqhkiG9w0BDAEDMA4ECFw78Uk8K64uAgIU+gQ4id0jRb3JyEM5fdpaeQR+
YEeMn+Y5KavplVD5HtgQQY9hhppbQqG4af7KY+MT6xus6oNEQeJAE5wxPjAXBgkq
hkiG9w0BCRQxCh4IAGQAYQBuAGEwIwYJKoZIhvcNAQkVMRYEFEgDhsFpuHhtrt7z
zAawM6xXMt2WMC8wHzAHBgUrDgMCGgQUzSoHpcIerV21CvCOjAe5ZVhs2M8ECC5D
kkzl2MltAgIoAA==
-----END PKCS12-----

9. Security Considerations

The keys presented in this document should be considered compromised and insecure, because the secret key material is published and therefore not secret.

Any application which maintains a denylist of invalid key material should include these keys in its list.

10. IANA Considerations

IANA has nothing to do for this document.

11. Document Considerations

[RFC Editor: please remove this section before publication]

This document is currently edited as markdown. Minor editorial changes can be suggested via merge requests at https://gitlab.com/dkg/lamps-samples or by e-mail to the author. Please direct all significant commentary to the public IETF LAMPS mailing list: spasm@ietf.org

11.1. Document History

11.1.1. Substantive Changes from draft-ietf-*-07 to draft-ietf-*-08

* Apply editorial cleanup suggested during review

11.1.2. Substantive Changes from draft-ietf-*-06 to draft-ietf-*-07

* Correct document history

* Restore PKCS12 for dana and bob from -05

11.1.3. Substantive Changes from draft-ietf-*-05 to draft-ietf-*-06

* Added outbound references for acronyms PEM, CRL, and OCSP, thanks Stewart Brant.

* Accidentally modified PKCS12 for dana and bob

11.1.4. Substantive Changes from draft-ietf-*-04 to draft-ietf-*-05

* Switch from SHA512 to SHA1 as MAC checksum in PKCS#12 objects, for interop with Keychain Access on macOS.

11.1.5. Substantive Changes from draft-ietf-*-03 to draft-ietf-*-04

* Order subject/issuer DN components by scope.

* Put cross-signed intermediate CA certificates into PKCS#12 instead of self-signed root CA certificates.

11.1.6. Substantive Changes from draft-ietf-*-02 to draft-ietf-*-03

* Correct encoding of S/MIME Capabilities extension.

* Change "Certificate Authority" to "Certification Authority".

* Add CertificatePolicies to all intermediate and end-entity certificates.

* Add organization and organizational unit to all certificates.

11.1.7. Substantive Changes from draft-ietf-*-01 to draft-ietf-*-02

* Added cross-signed certificates for both CAs

* Added S/MIME Capabilities extension for Carlos and Dana's encryption keys, indicating preferred ECDH parameters.

* Ensure no serial numbers are negative.

* Encode keyUsage extensions in minimum-length BIT STRINGs.

11.1.8. Substantive Changes from draft-ietf-*-00 to draft-ietf-*-01

* Added Curve25519 sample certificates (new CA, Carlos, and Dana)

11.1.9. Substantive Changes from draft-dkg-*-05 to draft-ietf-*-00

* WG adoption (dkg moves from Author to Editor)

11.1.10. Substantive Changes from draft-dkg-*-04 to draft-dkg-*-05

* PEM blobs are now sourcecode, not artwork

11.1.11. Substantive Changes from draft-dkg-*-03 to draft-dkg-*-04

* Describe deterministic key generation

* label PEM blobs with filenames in XML

11.1.12. Substantive Changes from draft-dkg-*-02 to draft-dkg-*-03

* Alice and Bob now each have two distinct certificates: one for signing, one for encryption, and public keys to match.

11.1.13. Substantive Changes from draft-dkg-*-01 to draft-dkg-*-02

* PKCS#12 objects are deliberately locked with simple passphrases

11.1.14. Substantive Changes from draft-dkg-*-00 to draft-dkg-*-01

* changed all three keys to use RSA instead of RSA-PSS

* set keyEncipherment keyUsage flag instead of dataEncipherment in EE certs

12. Acknowledgements

This draft was inspired by similar work in the OpenPGP space by Bjarni Runar and juga at [I-D.bre-openpgp-samples].

Eric Rescorla helped spot issues with certificate formats.

Sean Turner pointed to [RFC4134] as prior work.

Deb Cooley suggested that Alice and Bob should have separate certificates for signing and encryption.

Wolfgang Hommel helped to build reproducible encrypted PKCS#12 objects.

Carsten Bormann got the XML sourcecode markup working for this draft.

David A. Cooper identified problems with the certificates and suggested corrections.

Lijun Liao helped get the terminology right.

Stewart Brant and Roman Danyliw provided editorial suggestions.

13. References

13.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <https://www.rfc-editor.org/info/rfc5958>.

[RFC7292] Moriarty, K., Ed., Nystrom, M., Parkinson, S., Rusch, A., and M. Scott, "PKCS #12: Personal Information Exchange Syntax v1.1", RFC 7292, DOI 10.17487/RFC7292, July 2014, <https://www.rfc-editor.org/info/rfc7292>.

[RFC7468] Josefsson, S. and S. Leonard, "Textual Encodings of PKIX, PKCS, and CMS Structures", RFC 7468, DOI 10.17487/RFC7468, April 2015, <https://www.rfc-editor.org/info/rfc7468>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/info/rfc8032>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8479] Mavrogiannopoulos, N., "Storing Validation Parameters in PKCS#8", RFC 8479, DOI 10.17487/RFC8479, September 2018, <https://www.rfc-editor.org/info/rfc8479>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/ Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/info/rfc8551>.

13.2. Informative References

[FIPS186-4] "Digital Signature Standard (DSS)", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.186-4, July 2013, <https://doi.org/10.6028/nist.fips.186-4>.

[I-D.bre-openpgp-samples] Einarsson, B. R., juga, and D. K. Gillmor, "OpenPGP Example Keys and Certificates", Work in Progress, Internet-Draft, draft-bre-openpgp-samples-01, 20 December 2019, <https://www.ietf.org/archive/id/draft-bre-openpgp-samples-01.txt>.

[RFC4134] Hoffman, P., Ed., "Examples of S/MIME Messages", RFC 4134, DOI 10.17487/RFC4134, July 2005, <https://www.rfc-editor.org/info/rfc4134>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/info/rfc5322>.

[RFC7469] Evans, C., Palmer, C., and R. Sleevi, "Public Key Pinning Extension for HTTP", RFC 7469, DOI 10.17487/RFC7469, April 2015, <https://www.rfc-editor.org/info/rfc7469>.

[RFC8410] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018, <https://www.rfc-editor.org/info/rfc8410>.

[RFC8418] Housley, R., "Use of the Elliptic Curve Diffie-Hellman Key Agreement Algorithm with X25519 and X448 in the Cryptographic Message Syntax (CMS)", RFC 8418, DOI 10.17487/RFC8418, August 2018, <https://www.rfc-editor.org/info/rfc8418>.

[SHA256] Dang, Q., "Secure Hash Standard", National Institute of Standards and Technology report, DOI 10.6028/nist.fips.180-4, July 2015, <https://doi.org/10.6028/nist.fips.180-4>.

[TEST-POLICY] NIST - Computer Security Divisiion (CSD), "Test Certificate Policy to Support PKI Pilots and Testing", May 2012, <https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/test_policy.pdf>.

Author's Address

Daniel Kahn Gillmor (editor)
American Civil Liberties Union
125 Broad St.
New York, NY, 10004
United States of America

Email: dkg@fifthhorseman.net